77

THE

MESSENGER OF MATHEMATICS.

EDITED BY

J. W. L. GLAISHER, Sc.D., F.R.S.,

FELLOW OF TRINITY COLLEGE, CAMBRIDGE.

VOL. XLI.

[MAY 1911—APRIL 1912].

Cambridge: BOWES & BOWES.

London: MACMILLAN & CO. LTD.

Glasgow: JAMES MACLEHOSE & SONS.

1912.

CONTENTS OF VOL. XLI.

MESSENGER OF MATHEMATICS.

DETERMINATION OF SUCCESSIVE HIGH PRIMES

[Fourth Paper].

[*Shewing* 696 *new high primes*].

By *Lt.-Col. Allan Cunningham, R.E*, Fellow of King's College, London.

[The author is indebted to Mr. H. J. Woodall, A.R.C.Sc., for reading the Proof sheets of this Paper.]

29. *Scope of Paper.* This Paper is in continuation of *three* previous Papers with same title in this Journal, viz.

Vol. xxxi., 1902, pp. 165–176; Vol. xxxiv., 1905, pp. 72–89, and 184–192;

and the numbering of the Articles, Examples, and Tables in the present Paper is in continuation of the numbering in the third Paper.

29*a*. *High Numbers and Primes.* Most of the numbers (N) dealt with in this series of Papers are* $> 10^7$, and may therefore be termed *High Numbers*, being beyond the limit of the present large Factor Tables. Those which are prime may be termed *High Primes*, as their primality cannot be detected from those Tables.

The Method here used for factorising the *whole of* the High Numbers (N) within a given "Range," say from (N_0-b) to (N_0+b'), and for determining the *whole of* the High Primes in that "Range," is fully explained in Art. 1–5 of the first Paper (Vol. xxxi.): but, to render the present Paper easily intelligible by itself, a brief outline of the process is here given again.

30. *Factorising Method.* Let N_0 be any high number whose Residues $(+R, -R')$ upon division by the *whole succession* of primes $p=3, 5, 7, \ldots$, up to $\sqrt{(N_0)}$ and powers of primes $p^\kappa=9, 25, 27$, &c., ..., up to $\sqrt{(N_0)}$ have been

* In the second of these Papers, Vol. xxxiv., pp. 72–75, two groups of numbers $N > 9.10^6$, both $< 10^7$, were dealt with. These were *at that time* (1904) beyond the power of the *then* existing Factor-Tables, so were then styled *High Numbers*, and *High Primes* (when prime). Dr. Lehmer's large Factor-Tables, which extend a little beyond 10^7, were only published in 1910.

calculated. Then $(N_0 - R)$, $(N_0 + R')$ are the two numbers nearest to the "Central Number" N_0 (one $< N_0$, and one $> N_0$), which are exactly divisible by p or p^κ. And *all* the numbers (N), exactly divisible by p, or p^κ, are given by the general formulæ—

$$N = N_0 - (mp + R) \equiv 0, \quad N = N_0 + (mp + R') \equiv 0 \pmod{p},$$

$$N = N_0 - (mp^\kappa + R) \equiv 0, \quad N = N_0 + (mp^\kappa + R') \equiv 0 \pmod{p^\kappa}.$$

If all the numbers (N) within the chosen "Range" $(N_0 - b')$ to $(N_0 + b')$ be entered in a Table, and all the divisors (p, p^κ)—found as above—up to the limit p and $p^\kappa \not> \sqrt{(N_0 + b')}$ be entered against each, then this process ends in disclosing *all the composite* numbers within the Range, together with all their factors $< \sqrt{N}$, and the residual factor (if any) may be found by dividing out the already known factors. Also, the numbers (N) for which no factors are found are hereby shown to be prime.

31. *Least Factor Tables.* The Tables with this name herewith printed show in general—so far as the column-width (5 figures) admits—the following data for each of the numbers N within the "range."

(1) The *least* prime factor (usually >5, but) $< \sqrt{N}$.

(2) Powers of the least prime factor are shown thus :—
- (*a*) Powers of 7 by 49, 343, 2401. Powers of 11 by 121, 1331.
- (*b*) The letters *s*, *c*, *f* after a factor denote that that factor appears in the *square* or *cube*, or *fourth* power respectively.

(3) The next higher (prime) factor is also shown if space admits.

(4) The letter *q* shows that the remaining factor is a prime ($< 10^7$).

(5) The letter *Q* shows that the remaining factor is a High Prime ($> 10^7$).

(6) The letters *d*, *t* show that the remaining factor is a product of *two* or *three* primes; [*d* for *two*, *t* for *three*].

(7) The least factors 3 or 5 are usually omitted (as their existence is easily recognisable) in order to make room for factors >5 (the insertion of which is deemed more useful).
The factors 3, 5, and their powers, are however inserted when the only other entry is *q* or *Q* : as in these cases there is plenty of room, and the information is useful.

8. The letter *p* shows that the number in question is itself a High Prime.

The data thus given suffice in most cases (*i.e.* except when the letters *d*, *t* occur) for the *complete resolution* of the com-

posite numbers N into their prime factors *without further reference* to Tables; and suffice in all cases to reduce them within the powers of the large Factor Tables.

32. *Example* 8°. $N = (2^{27} \mp R)$. The number here chosen as "Central Number" is $N_0 = 2^{27}$, and the "Range" chosen is the group of 2000 numbers from $(2^{27} - 1000)$ to $(2^{27} + 1000)$. The search for factors (Art. 30) was done by aid of the *Binary Canon Extension* described below (Art. 38).

32*a*. *Least Factor Tables* (Tab. XII*a*, *b*). These Tables give for all the *odd* numbers (N) within the "Range" some of the data described in Art. 31—(1) to (8). The Argument ($R = 10m + r$) of these Tables is shown thus:

The value of m (*i.e.* the hundreds and tens digits of R), in left columns.

The value of $r = 1, 3, 5, 7, 9$ (*i.e.* the units digit of R) in top-line.

[The *even* numbers within the Range are all *omitted*, inasmuch as after division by 2, 4, 8, they fall within the "Ranges" treated of in the previous Papers, and division by 16 brings them within the power of the large Factor-Tables].

32*b*. *Algebraic Factorisation.* In a few cases the numbers N are algebraically resolvable, *e.g.*

$$N = 2^{27} \mp y^3 = (2^9 \mp y)(2^{18} \pm 2^9.y + y^2); \quad y = 3,\ 5,\ 7,\ 9].$$

$$N = 2^{27} \mp 2^5 - 1 = (2^9 \pm 2^5 + 1)(2^{18} \mp 2^{14} + 2^9 - 1).$$

32*c*. *High Primes.* These are primes of the form

$$p = \tfrac{1}{\mu}.N = \tfrac{1}{\mu}.(2^{27} \mp R) > 10^7; \quad [\mu = 1,\ 3,\ 5,\ 7,\ 9,\ 11,\ 13].$$

They are shown in the Least Factor-Tables (Tab. XII*a*, *b*) by the letters p, Q; and are collected together in the Table below.

The Abstract below shows the number (n) of High Primes (p) found within the "Range" for each value of μ: the last line shows the approximate magnitude of each class in millions (M denotes *one* million).

$\mu =$	1	3	5	7	9	11	13	*Total*
$n =$	110	36	21	19	16	11	8	221.
p near	$134 M$	$44\frac{3}{4} M$	$26\frac{1}{5} M$	$19\frac{1}{6} M$	$14\frac{9}{10} M$	$12\frac{1}{5} M$	$10\frac{1}{3} M$	

Most of these primes are believed to be *new*, *i.e.* hitherto* unpublished (so far as known to the author).

* Three will be found in a Paper (by the present author and Mr. H. J. Woodall jointly) in Vol. XXXVII. of this Journal, p. 82.

List of 221 *High Primes* $p = \frac{1}{\mu}.N$: *between* $N = (2^{27} \mp 1000)$: $[\mu = 1$ *to* $13]$

$\mu = 1$					$\mu = 3$		$\mu = 5$	$\mu = 7$	$\mu = 9$	$\mu = 11$
134,21...					44,73...		26,84...	19,17...	14,91...	12.20...
6729	7079	7493	7943	8391	8927	9421	3347	3821	2977	1557
6737	7089	7497	7973	8397	8959	9449	3419	3827	2983	1583
6759	7103	7509	7977	8421	8987	9491	3437	3839	3011	1587
6777	7131	7539	7989	8423	9007	9503	3441	3871	3013	1593
6783	7157	7541	8031	8429	9059	9511	3471	3887	3023	1599
6791	7163	7593	8037	8433	9089	9521	3491	3899	3037	1611
6801	7173	7613	8039	8459	9113	9533	3497	3911	3049	1619
6807	7199	7617	8057	8463	9139	9551	3503	3919	3079	1643
6827	7221	7649	8069	8481	9151	9553	3513	3923	3103	1659
6837	7247	7689	8081	8493	9157	9557	3521	3929	3121	1671
6861	7257	7757	8103	8537	9173	9559	3543	3949	3127	1677
6867	7277	7773	8153	8549	9181	9571	3549	3967	3161	
6869	7301	7779	8159	8627	9259		3563	4003	3169	$\mu = 13$
6881	7323	7781	8169	8703	9269		3581	4007	3179	
6899	7353	7799	8171		9271		3587	4013	3181	10,32...
6911	7361	7803	8181		9311		3623	4031	3187	
6933	7367	7823	8199		9313		3651	4033		4367
6939	7401	7827	8237		9329		3657	4037		4393
6947	7403	7869	8243		9341		3669	4093		4399
6987	7409	7877	8289		9353		3699			4409
7001	7437	7893	8291		9361		3743			4427
7043	7439	7917	8303		9371					4459
7047	7467	7929	8307		9391					4507
7049	7487	7931	8327		9397					4513
Total Number ...			...	110	...	36	21	19	16	11 & 8

32*d*. *Highest Consecutive Primes.* It is interesting to note that the 110 highest primes here reported (from 134216729 onwards) are believed to be the *highest consecutive primes* known.

32*e*. *Highest Composite Mersenne's Numbers.* If $M_q = (2^q - 1)$ be a *Mersenne's Number* (*i.e.* q = prime), and $q = 4k + 3$; and if $p = (2q + 1) = (8k + 7)$ be also prime; then $M_q \equiv 0 \pmod{p}$ always. The Tables of primes $p = (2^{26} \mp R)$, and $(2^{27} \mp R)$, given in the third of these Papers and in the present one, give three such *composites* M_q; these are believed to be the highest composite Mersenne's Numbers known.

Ex.			
	$q =$ 67108623	67108683	67109051
	$p =$ 134217247	134217367	134218103

33. *Example* 9°. $N = (3^{16} \mp R)$. The number (N_0) here chosen as "Central Number" is $N_0 = 3^{16}$, and the "Range" chosen is the group of 2160 numbers from $(3^{16} - 1080)$ to $(3^{16} + 1080)$. This work has been rendered possible by the aid of a *Ternary Canon* described below (Art. 38).

[The work of $N = (3^{15} \mp R)$, which forms Example 3° of the first of these Papers (Art 8), depended at the time on Mr. Woodall's work only (as stated in Art. 9): it has been recently examined by one of Col. Cunningham's Assistants, and *found correct* throughout].

33*a*. *Least Factor Tables* (Tab. XIII., XIV., XV.) Three Tables are provided, giving, for all the *odd* numbers N, $\frac{1}{2}N$, $\frac{1}{4}N$ within the "Range" $N=(3^{16}\mp 1080)$ not divisible by 3 or 5, some of the data described in Art. 31—(1) to (8).

The Argument (R), which differs in the three Tables, is as follows:

$$N\left\{\begin{array}{c|c} R=(30m+r) & R'=(30m+r') \\ r=28,\ 22,\ 20,\ 14,\ 10,\ 8,\ 4,\ 2 & r'=2,\ 8,\ 10,\ 16,\ 20,\ 22,\ 26,\ 28, \end{array}\right.$$

$$\tfrac{1}{2}N\left\{\begin{array}{c|c} R=(60m+r) & R'=(60m+r') \\ r=59,\ 55,\ 47,\ 43,\ 35,\ 23,\ 19,\ 7 & r'=1,\ 5,\ 13,\ 17,\ 25,\ 37,\ 41,\ 53, \end{array}\right.$$

$$\tfrac{1}{4}N\left\{\begin{array}{c|c} R=(120m+r) & R'=(120m+r') \\ r=109,\ 85,\ 77,\ 53,\ 37,\ 29,\ 13,\ 5 & r'=11,\ 35,\ 43,\ 67,\ 83,\ 91,\ 107,\ 115. \end{array}\right.$$

The values of r, r' above are arranged so that

Tab. XIII. of N. N shall not contain 2, 3, 5.

Tab. XIV. of $\frac{1}{2}N$. N shall contain 2, but not 4, 3, 5.

Tab. XV. of $\frac{1}{4}N$. N shall contain 4, but not 8, 3, 5.

The portion $30m$, $60m$, $120m$ of the Argument R is placed in the left columns, and the portion r, r' is placed in the head-line, in all the Tables.

[The numbers N divisible by 3 are *omitted*, inasmuch as (after division by 3) they fall within the Range $(3^{15}+R)$ worked out in Ex. 3° in the first of these Papers (Vol. XXXI, pp. 170, 171). Those divisible by 5 are *omitted*, because (after division by 5) they fall within the powers of the large Factor-Tables].

33*b*. *Algebraic Factorisation.* In a few cases the numbers N are *algebraically* resolvable into two, or more, co-factors, *e.g.*

$N=(3^{16}-y^2)=(3^8-y)(3^8+y)$; $[y=2, 4, 8, 10, 14, 16, 20, 22, 26, 28, 32]$.

$N=(3^{16}+4y^4)=(3^8-2.3^4y+2y^2)(3^8+2.3^4y+2y^2)$; $[y=2, 4]$.

33*c*. *High Primes.* These are primes ($>10^7$) of the form

$$p=N=(3^{16}\mp R),\quad p=\tfrac{1}{2}N=\tfrac{1}{2}(3^{16}\mp R),\quad p=\tfrac{1}{4}N=\tfrac{1}{4}(3^{16}\mp R).$$

They are shown in the Least Factor-Tables (Tab. XIII. to XV.) by the letter p, and are collected together in the Table below.

The Abstract below shows the number (n) of each class found, and their approximate magnitude in millions (M denotes *one* million).

$p=$	$(3^{16}\mp R)$	$\frac{1}{2}(3^{16}\mp R)$	$\frac{1}{4}(3^{16}\mp R)$	*Total*
$n=$	114	58	28	200
p near	$43M$	$21\frac{1}{2}M$	$10\frac{3}{4}M$	

These primes are believed to be all *new*, *i.e.* not hitherto published* (as far as known to the author).

List of 114 *High Primes* $p = N$ *between* $(3^{16} \mp R)$.

43,045...			43,046...						43,047...				
.	759	927	027	167	299	579	749	957		113	271	503	643
.	771	939	033	173	309	581	779	959		139	307	541	679
663	781	943	071	203	323	587	789	963		149	353	547	691
669	823	957	083	209	371	599	831	981		157	379	551	703
679	841	969	111	221	401	603	807		001	161	401	569	707
693	883	973	117	233	467	611	909		013	197	439	583	721
711	901	979	137	257	477	617	911		047	209	457	611	731
727	907	991	149	279	537	623	923		091	239	461	617	737
729	909	997	161	291	543	747	953		097	269	497	619	

List of 58 *High Primes* $p = \frac{1}{2}N$ *between* $\frac{1}{2}(3^{16} \mp R)$.

21,522...			21,523...										
829	889	947	001	093	273	351	399	499	543	591	669	739	793
859	911	961	049	171	277	361	417	511	571	609	679	741	813
881	923	971	063	261	283	387	421	519	573	631	681	753	847
887	931	989	069	267	339	391	433	531	589	651	727	763	891
												769	897

List of 28 *High Primes* $p = \frac{1}{4}N$ *between* $\frac{1}{4}(3^{16} \mp R)$.

10,761...													
431	469	521	547	589	649	671	701	719	767	841	869	889	937
451	517	529	563	601	661	689	713	763	827	851	887	899	941

34. *Example* 10°. $N = (5^{11} \mp R)$. The number here chosen as "Central Number" is $N_0 = 5^{11}$, and the "Range" chosen is the group of 2040 numbers from $(5^{11} - 1020)$ to $(5^{11} + 1020)$. The search for factors (Art. 30) was done by aid of a *Quinary Canon* described below (Art. 38).

34*a*. *Least Factor Tables.* (Tab. XVI.-XIX.).

Four Tables are provided, giving, for all the *odd* numbers N, $\frac{1}{2}N$, $\frac{1}{3}N$, $\frac{1}{4}N$ within the "Range" $N = (5^{11} \mp 1020)$ not divisible by 3 or 5, some of the data described in Art. 31—(1) to (8).

* One of these $p = 21523361 = \frac{1}{2}(3^{16}+1)$ was determined to be prime many years ago by the late Mr. Chas. E Bickmore, and the present author, and also by Mr Morgan Jenkins.

The Argument (R), which differs in the four Tables, is as follows:

N	$R=(30m+r)$ $r=28, 24, 22, 18, 16, 12, 6, 4$	$R'=(30m+r')$ $r'=2, 6, 8, 12, 14, 18, 24, 26,$
$\frac{1}{2}N$	$R=(60m+r)$ $r=51, 43, 39, 31, 27, 19, 7, 3$	$R'=(60m+r')$ $r'=9, 17, 21, 29, 33, 41, 53, 57,$
$\frac{1}{3}N$	$R=(90m+r)$ $r=86, 68, 62, 44, 32, 26, 14, 8$	$R'=(90m+r')$ $r'=4, 22, 28, 46, 58, 64, 76, 82,$
$\frac{1}{4}N$	$R=(120m+r)$ $r'=97, 81, 73, 57, 49, 33, 9, 1$	$R'=(120m+r')$ $r'=23, 39, 47, 63, 71, 87, 111, 119,$

The values of r, r' are so arranged that

Tab. of N	Tab. of $\frac{1}{2}N$	Tab. of $\frac{1}{3}N$	Tab. of $\frac{1}{4}N$
$N \neq 2n, 3n, 5n$	$\frac{1}{2}N \neq 2n, 3n, 5n$	$\frac{1}{3}N \neq 2n, 3n, 5n$	$\frac{1}{4}N \neq 2n, 3n, 5n.$

The portion $30m$, $60m$, $90m$, $120m$ of the Argument R is placed in the left column, and the portion r, r' is placed in the head-line of all the Tables.

[Numbers divisible by 5 are *omitted*, inasmuch as—after division by 5—they fall within the 10th million, and are thus within the power of the new* large Factor-Tables].

34*b*. *High Primes*. These are primes ($> 10^7$) of the forms

$$p = \tfrac{1}{\mu} . N = \tfrac{1}{\mu} . (5^{11} \mp R); \quad [\mu = 1, 2, 3, 4].$$

They are shown in the Least Factor-Tables (Tab. XVI. to XIX.) by the letter p, and are collected together in the Table below.

The Abstract below shows the number (n) of High Primes (p) found within the "Range" for each value of μ: the last line shows the approximate magnitude of each class in millions (M denotes *one* million).

$\mu =$	1	2	3	4	*Total*
$n =$	132	69	37	37	275
p near	$48\frac{1}{3}M$	$24\frac{2}{3}M$	$16\frac{1}{4}M$	$12\frac{1}{3}M$	

These primes are believed to be all *new*, *i.e.* not hitherto published (so far as known to the author).

35. *Tests of Work*. Same as in Art. 9 of first Paper, *q. v.*; also add—

Ex. 8°, 9°, 10°. The whole of the numerical work has been worked out by two† computers *independently* (under the author's close supervision): the results were then collated, and all discrepancies were examined by both and brought to agreement.

---

* Dr. Lehmer's, which extend up to a little beyond 10^7.

† Mr. R. F. Woodward and Miss A. Woodward.

List of 275 High Primes $p = \frac{1}{\mu} . N$ *between* $N = (5^{11} \mp 1080)$.

$[\mu = 1, 2, 3, 4]$.

$\mu=1$				$\mu=2$		$\mu=3$	$\mu=4$
48,82...				24,41...		16,27...	12,20...
	7539	8173	8679	3531	4149	5691	6773
	7557	8181	8737	3579	4157	5703	6791
	7567	8187	8739	3593	4161	5709	6827
	7579	8203	8757	3617	4199	5733	6833
	7591	8209	8797	3629	4209	5769	6849
	7617	8217	8821	3663	4217	5793	6851
	7629	8229	8823	3671	4223	5797	6861
	7641	8259	8851	3677	4233	5821	6869
7063	7671	8277	8859	3681	4241	5859	6879
7069	7683	8289	8869	3693	4281	5901	6897
7071	7699	8293	8881	3699	4283	5911	6899
7081	7711	8331	8883	3729	4301	5923	6939
7099	7741	8359	8887	3731	4319	5937	6989
7101	7771	8361	8889	3749	4323	5949	6993
7113	7773	8371	8907	3759	4337	5971	7007
7117	7789	8389	8919	3773	4349	5977	7011
7143	7809	8391	8943	3777	4361	5979	7017
7147	7819	8401	8971	3783	4371	5991	7023
7153	7837	8407	8973	3791	4409	6031	7029
7189	7881	8433	8979	3801	4451	6079	7031
7221	7921	8449	9007	3827	4461	6087	7047
7227	7941	8457	9009	3843	4463	6129	7049
7239	7951	8467	9013	3863	4473	6151	7067
7243	7953	8469	9019	3891	4493	6171	7079
7249	7963	8473	9093	3899	4517	6177	7121
7297	7969	8491	9133	3903	4521	6201	7127
7369	7983	8497	9141	3947	4527	6213	7179
7371	7993	8511	9181	3953	4529	6223	7187
7381	8037	8541	9201	3959	4541	6237	7191
7393	8041	8553		3999	4571	6277	7193
7419	8047	8569		4011	4587	6289	7197
7453	8053	8589		4037	4589	6297	7203
7479	8079	8599		4041		6307	7229
7483	8107	8601		4053		6319	7269
7497	8113	8623		4059		6343	7271
7507	8139	8631		4113		6349	7287
7533	8163	8671		4121		6391	7301
Total Number	...	...	132	...	... 69	37	37

36. *Sequences of Composites.* Add to previous Art. 11, 19, 25, the following *long sequences of composite numbers* (without any prime intervening).

	Between the primes		*Between the primes.*
77;	21523093—21523171.	77;	44739181—44739259.
89;	21523171—21523261.	77;	134218549—134218627.
73;	48829019—48829093.	75;	134218627—134218703.

37. *Distribution of Primes.* Add to previous Art. 12, 20, 26, the following numbers (n) of primes within the "Range" of 1000 numbers from ($N_m - 1000$) to N_m.

$$N_m = 3^{16},\ n = 55;\quad N_m = 5^{11},\ n = 56;\quad N_m = 2^{27},\ n = 58.$$

38. *Prime-pairs.* Two primes (p, q) whose difference $p \sim q = 2$ are sometimes called a *Prime-pair*. The following Abstract shows the number (n') of prime-pairs in the "Ranges" from ($N_0 - R$) to ($N_0 + R$) named below, and also the total number (n) of primes in the same "Ranges."

$N_0 =$	$\frac{1}{4}3^{16}$, $\frac{1}{2}3^{16}$, 3^{16}	$\frac{1}{4}\cdot5^{11}$, $\frac{1}{3}\cdot5^{11}$, $\frac{1}{2}5^{11}$, 5^{11}	$\frac{1}{13}2^{27}$, $\frac{1}{11}\cdot2^{27}$, $\frac{1}{9}2^{27}$, $\frac{1}{7}2^{27}$, $\frac{1}{5}2^{27}$, $\frac{1}{3}2^{27}$, 2^{27}
$R =$	270, 540, 1080	270, 360, 540, 1080	77, 91, 111, 143, 200, 333, 1000
$n' =$	1, 5, 8	6, 1, 5, 15	0, 0, 2, 1, 0, 4, 11
$n =$	28, 58, 114	37, 37, 69, 132	8, 11, 16, 19, 21, 36, 110

Comparing these figures with those in Art. 21, 27 tends to confirm Dr. Glaisher's statements* that (1) the percentage of prime-pairs (in a large range of numbers) decreases on the whole as the numbers increase in magnitude, and (2) that n' is generally $< \frac{1}{10}n$.

[*Highest prime-pairs.* The 11 prime-pairs between ($2^{27} \mp 1000$) are believed to be the *highest prime-pairs* known).

39. *Arithmetical Canons.* The search for factors described above has been rendered possible by the construction of the three Arithmetical Canons described below:—

Binary Canon† *Extension.* This gives the Residues (both $+R$, $-R$) of 2^x up to $x = 100$ on division by all primes (p) and prime-powers (p^κ) up to 10000: and also up to $x = 36$ on division by all primes (p) and prime-powers (p^κ) up to 12000.

Ternary and Quinary† *Canons.* These give the Residues (both $+R$, $-R$) of 3^x and 5^x up to $x = 16$ on division by all primes (p) and prime-powers (p^κ) up to 10000; and in some cases up to higher limits of both x and p.

---

* See pp. 28, 31 of Dr. Glaisher's Paper, *An Enumeration of Prime-pairs*, in Vol. VIII. of this Journal.

† The three Canons were computed throughout by Miss A. Woodward, under the present author's superintendence. The Binary and Ternary Canons have been also computed (independently) by Mr. H. J. Woodall. The two copies of each have been collated. The three Canons have been in constant use in searching for factors, and have thereby received much indirect verification. They are at present only in M.S.; but it is hoped to publish the Binary shortly.

Least Factors of $N = (2^{27} - R)$; $[R = 10m + r]$.

TAB. XII*a*.

m	r: 9	7	5	3	1	m	r: 9	7	5	3	1
99	p	11d	49q	5Q	p	49	131q	41d	43d	19q	7.11d
98	41q	19q	269q	13.67	7Q	48	13d	37q	179q	709q	p
97	181d	17q	11.23	463q	81q	47	29q	7.89d	53q	3.5q	p
96	p	7d	31d	3701q	71d	46	11.23	17q	61d	7.13sq	3Q
95	1747q	13Q	2131q	7.11d	p	45	107q	59d	19sq	929q	p
94	19d	3Q	p	17.29	223d	44	7.431	11.67	127q	3.5q	79q
93	7Q	p	9Q	4297q	11.13	43	47.73	13q	7Q	17q	163q
92	23.59	p	7.43d	607q	p	42	6317q	p	11d	23d	7.29d
91	761q	27q	79q	271q	7.19d	41	823q	19d	41q	37q	13Q
90	11.17	41q	13d	31q	p	40	43q	49.31	p	11d	337q
89	53sq	49q	4993q	3.5q	p	39	17d	599q	9Q	7.71q	311q
88	6577q	11d	29d	7.23d	9Q	38	3Q	199d	13d	3.5q	11d
87	13d	73q	17d	5.19d	757q	37	7.19q	23sq	p	5Q	271q
86	7.331	p	11.97	27.5q	p	36	53q	p	7.17d	29q	p
85	p	37d	7Q	13q	3Q	35	11.13	383q	349q	125q	7Q
84	67q	p	883q	11d	7.17d	34	173q	239q	31.47	61d	19q
83	43d	23q	19.83	89q	61q	33	37.59	7.11d	137q	13.41	17.23
82	p	7.13d	41d	421q	11q	32	167q	p	p	7.43q	151q
81	71q	p	47q	7.647	59sq	31	p	193q	11Q	67d	3Q
80	729q	17q	461q	3.25q	13sq	30	49d	13d	29q	19q	139d
79	343d	19d	p	53q	23q	29	89q	17d	7Q	121d	p
78	p	8681q	7.199	37d	p	28	p	9Q	23d	31.79	7.13q
77	31q	121q	13d	17q	7.877	27	11119	1297q	3Q	5Q	11Q
76	29d	3Q	373d	149d	131d	26	27q	7Q	19.37	17.53	p
75	19d	7.79d	11q	43q	1759q	25	5581q	3Q	13d	25.7q	41.47
74	13d	101d	23q	7.41q	p	24	11t	29d	107d	5Q	p
73	17q	853q	113q	11d	73d	23	7.23q	43d	p	9.5q	p
72	7.503	p	5849q	13q	19.47	22	13.17	11.19	7Q	557q	31.59
71	2753q	31q	7.67d	3.5q	11.29	21	p	563q	27q	5Q	49q
70	37.61	3Q	17d	193q	49q	20	3Q	331q	11Q	13q	499q
69	23d	13d	173q	59q	191q	19	p	9.7q	17q	23d	37d
68	11d	7.53d	p	19q	p	18	19.29	p	3Q	7.11q	571q
67	p	71q	263q	7.107	13.17	17	67d	13Q	233q	3.5q	83q
66	83d	11.43	673q	167q	41d	16	7.41q	149d	1321q	5Q	11.17
65	3.7q	4861q	31.89	23.29	7177q	15	31d	47.53	7.157	25q	13.19
64	p	81q	7.11t	197q	233q	14	263q	23.73	3709q	1019q	7.101
63	p	17sq	37q	5Q	7Q	13	11Q	1123q	p	2549q	29d
62	9Q	47q	p	11d	1181q	12	3923q	7.17d	13579	5Q	89q
61	13Q	7.181	1409q	4679q	9Q	11	227q	11.37	p	343d	p
60	137sq	19.23	601q	49.17	11Q	10	71q	27q	163q	59q	23q
59	79d	p	29q	13.31	103d	9	7.13d	31q	11q	17q	307q
58	7d	61q	73q	809q	43.53	8	97q	41q	7Q	3.5q	5783q
57	11.41	619q	7.59q	227q	p	7	p	1187q	19d	11.13	9.7q
56	17.19	13d	p	379q	7.23d	6	4969q	953q	43q	47d	137q
55	2287q	11d	p	2039q	3Q	5	17sq	7.113	23q	27t	121d
54	1621q	7d	101q	5Q	13Q	4	223q	13d	67d	7.37q	487q
53	27q	29t	121t	7.47q	19.31	3	p	19q	31q	109q	107q
52	p	467q	4211q	5Q	9Q	2	7.11q	457d	17q	139q	13d
51	7Q	11257	13.23	11q	313q	1	151d	9Q	49.29	5Q	4889q
50	113q	p	49q	83q	17q	.	23q	11Q	41.83	173q	7.73q

Least Factors of $N = (2^{27} + R')$; $[R' = 10m + r']$.

TAB. XII*b*.

m	r′ = 1	3	5	7	9	m	r′ = 1	3	5	7	9
·	19q	4057q	13t	2267q	17d	50	47q	7Q	2143q	29.79	p
1	199q	3.7q	11.59	5Q	421q	51	61q	6079q	p	7.281	17fq
2	43d	61q	131q	7.31d	p	52	11Q	31d	13d	5Q	2081q
3	13.37	71.79	2237q	11.23	19d	53	7Q	19d	3Q	43q	197q
4	7Q	17.29	p	2203q	3Q	54	27q	11.23	7.653	163q	37d
5	p	p	7.53q	13.89	11d	55	13sq	17q	5381q	5Q	7.491
6	101q	127q	1831q	3.5q	7.193	56	p	p	11.29	1069q	41q
7	p	191q	p	17.19	3Q	57	19d	49sq	p	13q	p
8	11Q	49.13	3Q	5Q	31 67	58	401d	73q	31.53	7.11d	23d
9	269q	1583q	p	7q	p	59	89d	6323q	47q	601q	p
10	29q	3.11q	37.97	43d	13d	60	7.71q	13d	59q	3.5q	11.19
11	7.17q	593q	19d	461q	9721q	61	107q	1163q	7d	5Q	3Q
12	409q	419q	7.11d	1543q	23d	62	17t	29.37	67q	2657q	7.13d
13	149d	59d	13d	347q	3.7q	63	11q	61q	23q	3.5q	701q
14	p	659q	17.61	11q	p	64	2503q	7.757	103q	19.31	243sq
15	31q	7 19q	3989q	1949q	29.41	65	41d	11Q	13 17	7d	83sq
16	13.53	643q	p	5.7q	11d	66	619q	p	79q	101q	p
17	271q	821q	23 71	5Q	17.37	67	49q	167q	121q	3083q	6143q
18	49q	107q	109q	13q	p	68	13.23	277q	7.19q	97q	17.47
19	121t	43q	7.379	443q	9Q	69	53q	p	p	11.37	7d
20	p	p	3Q	5Q	7.547	70	p	27q	p	13q	31.43
21	3Q	11.13	p	29q	47q	71	11197	7.271	241q	1753q	11Q
22	23d	7.67q	1609q	1051q	19q	72	9Q	17.19	1471q	7.23d	73d
23	179d	103d	11.89	7.827	13Q	73	p	13.41	p	1193q	29q
24	41d	3467q	p	17q	p	74	7.11d	71q	3Q	25q	3491q
25	7.59q	9.37q	139d	5.11q	3Q	75	1283q	p	7.61q	17d	13.67
26	p	101q	7.13d	19523	2719q	76	19d	11q	p	5Q	49.89
27	27q	337q	29.31	503q	49.11	77	31.37	23d	229q	1667q	257q
28	17d	151q	353d	131q	1931q	78	3Q	7.47q	11.13	157q	227q
29	13.73	7Q	3Q	1553q	97q	79	17q	9Q	43q	7 29d	19q
30	3.11q	p	19d	9.5.7q	p	80	599q	6911q	3Q	11d	p
31	p	23.47	17q	13.71	3347q	81	7.13d	911q	41d	3 5q	23d
32	7Q	11.41	81q	37.83	p	82	p	79q	7.17t	1103q	9.11q
33	3Q	29q	7.227	31sq	167d	83	181d	31q	3Q	13.19	7.109
34	p	13.19	11Q	863q	7 17d	84	59d	223sq	37q	113q	211q
35	2617q	p	3Q	67q	23q	85	11d	7.311	29q	1993q	17d
36	9Q	7Q	43d	11q	13.59	86	421q	13Q	23q	49q	101q
37	2069q	3.53q	p	49d	1487q	87	3Q	11d	19.73	47.61	463q
38	19q	17q	3Q	5Q	11.61	88	7.43d	9Q	71q	151d	13sq
39	7 29q	1303q	13d	107q	31d	89	557q	17.67	7.11d	41q	p
40	37sq	109q	7.23d	47d	199d	90	9Q	53d	967q	677q	7.563
41	11d	89d	9Q	5.17q	7 19q	91	23d	19.29	13d	121q	37q
42	13q	4999q	p	211q	149d	92	883q	7Q	3Q	17q	1657q
43	p	7.121	6421q	73q	103q	93	3Q	197d	709q	7q	11d
44	p	p	3Q	7.13q	29d	94	13Q	3Q	1031q	89d	3Q
45	17.23	p	11t	19q	71q	95	7.19q	379q	9Q	23 31	59q
46	7.31d	3Q	101q	479q	181q	96	11.17	937q	49d	13 43	853q
47	p	13d	49.37	5.11q	53q	97	29.47	81q	p	2207q	7.41q
48	647q	1237q	17d	41.59	7Q	98	79q	11d	3Q	5Q	19sq
49	67q	83 97	19d	23q	11.13	99	83d	7.13d	17d	3.25q	61q

Least Factors of $N=(3^{16}-R)$; $[R=30m+r]$.

30m	r: 28	22	20	14	10	8	4	2
1050	977q	17d	11.89	29d	911q	p	49.71	p
1020	11.23	p	7q	61d	13.67	p	19d	53q
990	4937q	7.43d	p	11.13	151q	7q	p	p
960	241q	11q	179q	251d	7.17d	167d	79q	p
930	31.37	13q	p	41q	p	11d	97q	157q
900	7q	3229q	2837q	7d	19.23	1291q	229q	17q
870	p	89d	29d	37.73	p	47q	13q	7.11d
840	17q	41q	191q	443q	1331q	13d	7q	197d
810	p	29d	7d	101q	p	23q	p	p
780	223q	7q	17q	p	61d	7d	11.47	p
750	p	23.31	13.71	p	49q	19d	43q	p
720	p	p	11.97	59d	p	107q	p	263q
690	7.11d	349q	31d	7.53q	337q	17.41	p	13q
660	p	19q	23.83	11q	233d	43.61	17d	49.37
630	29q	11d	p	19d	13d	p	7.23d	2579q
600	67.71	101d	7q	13d	p	121q	p	1163q
570	53q	7.73q	1613q	p	193q	7d	401q	p
540	19q	13517	p	p	7.109	p	827q	11.23
510	2333q	631q	19q	31q	11d	p	37.83	p
480	7q	47d	p	7.17d	79q	p	13.29	617q
450	191q	149d	2129q	p	175q	13q	11.19	7.41d
420	197q	p	37d	1995q	p	479q	7.61q	p
390	661q	p	7.11d	235q	31d	p	2347q	17q
360	11d	7q	13.59	5113q	41d	49.29	4507q	137d
330	17.23	97q	p	11.71	7.19d	31q	3433q	79d
300	13d	11q	p	47q	29q	653q	157d	13.19
270	7q	37q	17q	7q	53d	11d	4969q	4547q
240	271q	59q	491q	p	13d	2003q	p	7q
210	43q	2293q	3251q	135q	23.47	37d	7.31d	11q
180	3331q	71d	7q	29d	11d	17.19	p	83d
150	p	49.13	2659q	509q	523q	7.97q	17.73	31.43
120	839q	p	p	p	7d	23q	121d	p
90	p	19q	p	p	6551q	p	13d	67q
60	7.137	23d	11q	49.19	37q	13.53	6553q	467q
30	11.61	17q	281q	3217q	293q	2467q	103d	7.47q

Least Factors of $N=(3^{16}+R')$; $[R'=30m+r']$.

30m	r′: 2	8	10	16	20	22	26	28
·	195q	11d	7.13t	17q	43q	211q	p	p
30	443q	7.29d	19.41	797q	17d	7.11q	23d	p
60	13.47	p	1861q	461q	7q	71d	1993q	13d
90	59q	2971q	3469q	43q	p	163q	19q	121t
120	343d	107q	647q	7q	11.13	79q	p	23q
150	17.37	31d	331q	13q	733q	103q	67.89	7q
180	5107q	p	p	2633q	643q	p	7.11q	151q
210	29q	13q	49.17	37q	19.97	p	p	p
240	p	7d	11.47	449q	p	7.233	431q	19q
270	11d	43q	p	23.41	7.113	p	13q	1193q
300	439q	61q	67d	11.83	1483q	13.17	p	29.59
330	7.23q	11q	197q	7.859	173q	929q	17.53	3923q
360	199q	41d	p	p	5323q	11.19	29d	7.101
390	p	571q	13q	31d	1171q	883q	49q	p
420	149q	p	7.61d	p	p	1487q	59q	11.37
450	135d	7.17t	137q	4549q	11.23	7q	p	13d
480	83d	p	1303q	19q	7q	29q	691q	71q
510	281d	p	6337q	17q	13.31	41.47	11.43	547q
540	7d	p	p	7.13d	17.29	23q	6367q	53q
570	19q	67d	11q	p	101q	31q	37q	7q
600	121q	13.23	19d	79q	3889q	43d	7.47q	17q
630	p	157q	7q	11q	71q	1721q	1097q	p
660	17q	7.11d	37d	29q	p	7.59q	13.19	4271q
690	283q	1867q	23q	1321q	49.89	11.13	31q	p
720	73d	233q	17d	p	p	113q	23q	997q
750	7.617	109q	199q	7.761	107q	821q	p	11.31
780	p	4019q	135d	61d	11.19	6451q	6133q	2401q
810	97d	37d	p	p	p	17q	7.373	19.23
840	13d	p	7.29q	263q	41q	p	11.17	13.73
870	467q	7.227	43q	53d	p	7.37q	p	p
900	31q	29.47	11q	641q	7.13d	p	4201q	229d
930	11.79	409q	241q	13q	421q	19d	2393q	p
960	7q	17d	p	7.11t	67.83	p	p	701q
990	53q	11.13	p	97q	p	3593q	p	7.149
1020	23q	19q	401q	17.59	37.61	11d	7q	3257q

60m	r: 59	55	47	43	35	23	19	7
1020	661q	7.53q	41q	p	17.43	13.19	197q	431q
960	7.47q	11d	641q	p	37q	71q	23q	19q
900	p	4483q	p	p	7q	139q	17.29	343d
840	p	1193q	13.23	11.43	p	53q	p	37q
780	11q	13d	p	7q	19q	29.31	p	2089q
720	p	157q	7q	83d	103q	p	7.19d	79d
660	p	17q	11q	23d	67q	7.523	13.31	1553q
600	109d	7q	17d	49.97	613q	p	11d	61q
540	7q	p	19q	p	11.13	733q	3583q	151q
480	43d	p	4231q	13q	49d	1693q	137q	7.121
420	1201q	1439q	167d	811q	29.47	11.17	53.59	23.67
360	13q	71q	107q	7.37q	1913q	131q	p	13.43
300	195q	11q	7q	103q	23q	149q	49d	17.31
240	1013q	673q	191q	19d	113q	7.13q	2087q	41q
180	17q	7.199	53.73	11.29	181q	59q	p	p
120	7.11q	p	p	2063q	p	1453q	223q	2503q
60	61q	2861q	13.29	17q	7.79q	41q	47q	7.829
.	23.31	135d	11q	p	17q	43d	p	2707q

60m	r′: 1	5	13	17	25	37	41	53
.	p	761q	499q	7.347	1481q	683q	11.37	p
60	p	31.73	49q	p	11d	19q	7.13d	p
120	p	23cd	97q	1051q	p	7q	1427q	11.19
180	383q	7q	1973q	53d	13d	11.23	79q	83d
240	7.29d	41q	293q	13q	89d	p	251q	2239q
300	p	11.17	31q	p	7.19q	37d	p	7q
360	13d	p	17q	67q	193q	1877q	19.23	13q
420	p	p	1223q	7.11t	1627q	p	p	29q
480	1331d	37.47	7.23d	p	59d	13q	7.97q	2459q
540	p	271q	19q	2083q	83q	7.17q	p	263q
600	163q	7.787	11.61	p	4297q	p	p	1087q
660	49d	43d	13.47	23q	31q	431q	11d	17q
720	71q	13q	p	41q	7.11d	p	p	7q
780	17.19	p	281q	389q	p	p	29q	11.53
840	757q	2081q	79q	49.19	p	11d	13q	101d
900	41q	p	7.67q	17q	2999q	29q	7.73s	23q
960	233q	121q	p	59.89	13.17	7q	677q	599q
1020	1187q	7.503	349q	13q	23.53	31q	p	p

Tab XV.

Least Factors of $\frac{1}{4}N = \frac{1}{4}(3^{16} - R)$; $[R = 120m + r]$.

120m	r: 109	85	77	53	37	29	13	5
960	135d	1487q	11d	1361q	p	31q	61q	13q
840	7.11q	47d	p	7.281	109q	1931q	19q	p
720	67q	397q	43q	11.37	13.53	175d	569q	7q
600	607q	11d	347q	p	p	29q	49.17	p
480	311q	23q	7.59d	p	647q	11q	31.41	61q
360	p	7.13q	233q	2341q	19.29	7q	73q	p
240	971q	127q	p	67q	7q	89q	79q	121t
120	1069q	17q	23q	47d	11d	911q	13d	p
.	7.43q	59d	p	7.877	p	13q	23q	109q

Least Factors of $\frac{1}{4}N = \frac{1}{4}(3^{16} + R')$: $[R' = 120m + r']$.

120m	r′: 11	35	43	67	83	91	107	115
.	71q	p	1049q	17.29	p	53q	11q	7.37s
120	p	p	41d	277q	17.47	19.73	7q	43d
240	31d	103d	7.11t	223q	137q	p	p	23q
360	11q	7q	113d	509q	89q	7q	1395q	17d
480	13.41	19.53	173q	11q	49q	149q	p	13q
600	17d	11q	p	19q	p	101d	37q	97q
720	7.83q	p	29q	7q	13q	11d	p	p
840	457q	p	17q	13.23	43d	197q	383q	49.47
960	19q	29.31	37d	p	p	673q	7q	11q

Least Factors of $N = (5 - n)$; $[n = 30m + r]$.

30m	r = 28	24	22	18	16	12	6	4
1050	103q	7.13q	11q	1861q	43q	p	p	p
1020	13.17	p	179q	37q	1481q	7.19q	p	p
990	7.487	17q	p	p	11q	1613q	13d	19d
960	23d	11q	p	p	7.647	p	421q	37.59
930	2381q	3623q	257q	49d	17q	23q	p	7q
900	71q	31q	107q	11.13	151q	17.29	7.47q	p
870	p	43d	7.13q	131d	p	p	p	121d
840	53d	7q	31d	61q	41.89	11q	59q	17d
810	659q	73q	79d	p	211q	7q	37d	13sd
780	7.11d	19.23	83d	419q	29d	821q	11.71	5261q
750	173q	41q	6011q	2333q	7.19q	13.53	p	p
720	6569q	p	11.17	7.29d	13.61	p	1423q	7q
690	47q	223d	23d	17sd	p	1019q	7.307	191q
660	73q	13d	7q	89q	11.31	p	23d	239q
630	13q	49.11	19d	3511q	p	p	43.83	643q
600	p	47d	29d	p	2539q	7q	13.17	383q
570	7q	37d	p	11q	p	349q	19d	23q
540	p	29d	127q	p	49.97	31q	p	11q
510	17.19	p	337q	7.13t	521q	11d	79d	7q
480	p	17d	13.71	167q	p	59.61	7.113	p
450	11d	1867q	7q	67q	1427q	19d	11d	p
420	29d	7.53q	p	257d	17.23	173q	p	13.19
390	379q	p	11d	4987q	503q	7.17q	73q	743q
360	7.461	p	101q	43d	109q	13.37	31d	41d
330	79d	p	p	19sq	7.11d	47d	p	17.67
300	1259q	11q	89d	7q	p	151d	p	7.31d
270	23.37	13d	43q	p	1709q	41q	7q	29q
240	13d	509q	49q	11d	59q	23d	5323q	p
210	2153q	7.19q	17.53	1627q	2819q	443q	13.29	11q
180	2683q	p	571q	17d	19q	7.11d	239q	p
150	7.739	p	p	97q	3607q	p	p	47d
120	121q	89q	p	13559	7q	p	11.53	421q
90	31.41	23q	13q	7d	353q	131q	17q	7q
60	p	p	11.19	p	37.71	p	49.67	1319q
30	229q	127q	7.269	103q	p	29.79	41q	13.43
.	17d	7d	23q	p	11q	p	19d	61d

Least Factors of $N = (5 + n')$; $[n' = 30m + r']$.

30m	r′ = 2	6	8	12	14	18	24	26
.	331q	11.17	691q	859q	p	7.13d	23q	97q
30	49.19	1109q	p	73q	13d	p	233q	p
60	p	71q	31.67	11.37	7.17d	p	p	53q
90	p	13d	59d	7q	p	17.19	3691q	7.11t
120	13q	1571q	41.47	29q	p	11.43	7q	19.37
150	p	1061q	7.103	23sd	p	p	13q	17d
180	11d	7.373	73d	31.53	83q	1609q	11q	p
210	89d	59q	149q	19.47	43d	49d	p	p
240	7q	p	11.29	13q	23.31	1279q	p	p
270	1153q	p	13.17	p	7d	157q	37q	193d
300	563q	29d	p	7.17q	11q	163d	p	343q
330	p	121t	887q	p	p	p	7q	13q
360	61d	p	7.37q	p	19541	31q	271q	p
390	23q	7.43q	6367q	11d	53q	13q	17.97	p
420	29d	101d	p	79q	13d	7.23q	p	11q
450	7.59d	41d	5023q	3833q	p	11q	p	p
480	17.43	13d	19q	71d	7d	p	47d	p
510	11.13	17.37	4217q	49d	1277q	439q	11d	7q
540	359q	p	631q	971q	p	599q	7.13t	2551q
570	6857q	23d	7.121	1103q	17q	1069q	151q	29q
600	19d	7.61d	97q	p	p	17d	223q	31.73
630	p	1889q	617q	13q	11t	7q	29.43	479q
660	7.251	11q	13.23	p	347q	19q	131q	17q
690	47.83	p	p	41q	7.199	127q	23d	19q
720	53q	p	61q	7.11q	p	37.67	p	7.13d
750	1033q	p	p	p	p	139q	7d	11.71
780	p	47q	7.17d	19q	p	11.13	829q	23.59
810	31.37	49d	p	17q	13q	29.53	191q	839q
840	11q	p	p	23d	p	7.83d	11q	41q
870	7.67q	13sq	419q	p	p	p	p	151q
900	13q	19.79	11q	43d	49q	71.73	17.59	271q
930	109d	31q	3761q	7q	19.23	41q	13d	7q
960	127q	2011q	p	61q	11.47	283q	7q	233q
990	17q	11.97	7.31d	29d	107d	p	1847q	p
1020	2063q	7.17s	5443q	13d	37q	1123q	929q	139q
1050	311q	p	13.19	121q	73.79	7.47d	449q	p

Least Factors of $\frac{1}{2}N$, $\frac{1}{3}N$, $\frac{1}{4}N$. $N=(5^{11}\mp R)$.

$\frac{1}{2}N=\frac{1}{2}(5^{11}-R)$; $[R=60m+r]$. TAB. XVII. $\frac{1}{2}N=\frac{1}{2}(5^{11}+R')$; $[R'=60m+r']$.

	r									r'							
60m	51	43	39	31	27	19	7	3	60m	9	17	21	29	33	41	53	57
1020	67d	p	811q	19.83	47d	7.11d	53q	43.59	.	43d	11q	617q	131d	53q	107d	7.239	13.17
960	7.239	281d	29.71	331q	383q	41q	p	17q	60	149q	1291q	49.47	19d	23q	p	271q	p
900	11d	127q	p	13d	7.37q	23.61	11.73	239q	120	283q	7.71q	151q	11q	1877q	13.29	p	479q
840	p	29q	13d	7q	p	47d	97d	7.761	180	p	p	523q	2377q	13q	7.443	1171q	11q
780	31q	19d	11q	157q	773q	p	7.59q	p	240	7d	37q	17.73	47.67	p	11d	p	421q
720	p	p	7.17q	313q	19q	p	p	13q	300	p	13.19	p	17q	7.41d	p	43.79	p
660	541q	343d	853q	17q	11d	43q	p	p	360	11.13	547q	977q	7q	19.29	223q	11d	7q
600	29.41	11 23	1409q	37q	p	7.13q	p	53q	420	3083q	p	p	2713q	2341q	23d	49 13	p
540	7.641	31q	p	p	13q	p	1549q	p	480	193q	41d	7.11d	29q	p	p	17.31	67q
480	487q	p	19q	121q	49.43	3217q	17.41	37.47	540	p	7d	739q	179q	p	127q	137q	p
420	p	13d	23.31	7q	433q	p	967q	7.11q	600	83q	p	19q	13.59	11q	7q	317q	31.89
360	13.89	1151q	p	53d	83d	11d	7.19t	1621q	660	343t	11q	13d	197q	p	37q	4507q	673q
300	17q	p	7q	167q	p	p	139q	29q	720	101q	17.23	29d	409q	7.233	3037q	19q	p
240	11.19	7.17d	79q	3767q	67d	173q	11q	367q	780	61q	p	p	7.11q	3229q	p	47q	7.13q
180	p	613q	p	31q	p	7q	29.37	23d	840	19.37	29q	p	43q	17q	53d	7q	11d
120	7.163	43q	11.41	13d	17.71	19d	p	3547q	900	p	p	7.23q	p	p	1331t	353q	p
60	757q	p	13d	23d	7.31q	17.59	389q	19d	960	181q	7q	263q	41.71	13q	19q	23.89	p
.	p	p	37d	7 73q	121q	p	p	7.839	1020	11.31	521q	43d	p	p	49q	11.67	17.19

Least Factors of $\frac{1}{3}N$, $\frac{1}{4}N$. $N=(5^{11}\mp R)$.

$\frac{1}{3}N=\frac{1}{3}(5^{11}-R)$; $[R=90m+r]$. TAB. XVIII. $\frac{1}{3}N=\frac{1}{3}(5^{11}+R')$; $[R'=90m+r']$.

90m	r: 86	68	62	44	32	26	14	8	90m	r′: 4	22	28	46	58	64	76	82
990	191q	277q	p	23.89	13d	p	7.67q	p	.	7q	101q	11.83	7.41q	1531q	181q	257q	2579q
900	31d	83d	7.11q	13.97	317q	p	137q	2659q	90	121q	p	61q	p	13d	853q	557q	7d
810	11.23	7.17d	103q	29d	19d	7.613	563q	p	180	19q	67q	23.71	11.13	2459q	17q	7.227	p
720	1303q	13q	1663q	11q	49q	p	p	19.59	270	79q	11.41	7.19d	31.47	p	59.73	17.23	491q
630	661q	11d	41q	17.79	p	53q	71q	1871q	360	29d	7.13q	p	p	113q	49.11	827q	37d
540	7.131	463q	67q	7.101	17q	11d	13d	p	450	127q	1361q	p	109q	7q	p	19.83	307q
450	1093q	2837q	1013q	107q	23q	135d	43q	49q	540	p	2861q	43.89	p	47q	67d	13.53	11.23
360	37.41	31q	p	211q	p	19q	7.59q	11.17	630	7.71q	17d	2593q	7q	11.31	13q	p	29q
270	p	53q	7.29q	p	11d	197q	787q	p	720	523q	p	79d	p	1523q	41q	p	7.97q
180	17q	7.47d	13.31	37q	p	7.23d	p	p	810	149d	p	167q	17q	19q	31q	7 11t	883q
90	359q	19.29	p	2777q	7q	719q	11.73	3187q	900	p	p	7.13d	131q	17q	281q	2477q	19d
.	13d	23q	17q	19d	p	157q	433q	13d	990	2311q	2401q	11q	23q	p	7q	1031q	1931q

$\frac{1}{4}N=\frac{1}{4}(5^{11}-R)$; $[R=120m+r]$. TAB. XIX. $\frac{1}{4}N=\frac{1}{4}(5^{11}+R')$; $[R'=120m+r']$.

120m	r: 97	81	73	57	49	33	9	1	120m	r′: 23	39	47	63	71	87	111	119
960	23.29	61.97	p	11.31	13q	1487q	7q	p	.	17d	7.11d	23q	p	p	41d	83q	311q
840	19.43	53d	7q	41q	1361q	23q	461q	11d	120	p	175q	1327q	37d	p	7q	23q	13q
720	p	49.13	p	137q	31d	121d	p	p	240	7q	19.71	233q	11q	1637q	127d	53d	p
600	13q	p	2087q	17q	p	7.19q	p	107q	360	p	2503q	73q	61q	7.17d	13q	31q	11.37
480	7.11d	241q	61.83	p	p	2357q	11.13	19d	480	787q	2549q	101q	7q	13.47	11.17	p	7.23q
360	2207q	281q	59q	457q	49.37	2437q	p	29q	600	p	p	p	p	67d	p	7.389	31d
240	3461q	23d	11q	7q	71q	31d	17.43	7.41q	720	11.41	13d	49q	23.43	p	163q	11q	17d
120	953q	47q	211q	13.19	p	p	7.29q	79d	840	13q	7.103	19q	199q	61d	47d	p	p
.	p	p	7.13d	p	11d	p	p	p	960	59d	3407q	11d	p	29q	7.151	13.37	p

NOTE ON A THEOREM OF CESÀRO.

By *G. H. Hardy*.

1. ON p. 53 of his *Introduction to the Theory of Infinite Series* Dr. Bromwich states and proves the following theorem:

Let a_n be a positive and steadily decreasing function of n, whose limit, as $n \to \infty$, is zero; and let p_n be the number of positive terms and q_n the number of negative terms in the first n terms of the series

$$\pm a_1 \pm a_2 \pm a_3 \pm \ldots, \tag{1}$$

so that $p_n + q_n = n$. Then if the series (1) *is convergent, but not absolutely convergent, the ratio*

$$p_n / q_n$$

cannot tend to any limit other than unity—or, what is the same thing, the ratio

$$(p_n - q_n)/n$$

cannot tend to any limit other than zero.

The theorem is due to Cesàro (*Rendiconti della Accademia dei Lincei*, ser. 4, t. 4, p. 133). The proof given by Dr. Bromwich is based upon one given by Bagnera (*Bulletin des Sciences Mathématiques*, sér. 2, t. 12, p. 227).

I find that Cesàro proved a good deal more than this; and, as the theorem in question is an exceedingly curious and interesting one, I think it may be worth while to make a few remarks about it.

2. The theorem itself assigns no criterion for the existence of the limit p_n/q_n; it merely states that *if* it exists it must be unity. Cesàro, however, went on to consider the question of the existence of the limit, and in the paper already quoted states the further result: "*If the series Σa_n is not less divergent than the harmonic series, i.e., if na_n is ultimately greater than some positive constant, then p_n/q_n certainly tends to a limit (that is to say, unity).*"

The proof that he gives appears, however, to be faulty.*

* See the argument (*l.c.*, p. 135) beginning "S' il est impossible de trouver..." : and that beginning " En effet, si $(\epsilon_1 + \epsilon_2 + \ldots + \epsilon_n)/n$ n'admet pas une limite..."

Cesàro, however, returned to the subject in a later paper (*Nouvelles Annales*, sér. 3, t. vii., p. 405), and gave a valid and much simpler proof as follows. Let

$$u_n = \pm a_n = \epsilon_n a_n, \quad s_n = u_1 + u_2 + \ldots + u_n.$$

Then, as $n \to \infty$, $s_n \to s$, say; and by a well-known theorem of Cauchy and Stolz, if A_n is a function of n which tends steadily to infinity with n, we have

$$\frac{A_1 s_1 + (A_2 - A_1) s_2 + \ldots + (A_n - A_{n-1}) s_n}{A_n} \to s,$$

or

$$s_n - \frac{A_1 u_2 + A_2 u_3 + \ldots + A_{n-1} u_n}{A_n} \to s,$$

or

$$\frac{A_1 u_2 + A_2 u_3 + \ldots + A_{n-1} u_n}{A_n} \to 0.$$

But also, as $u_n \to 0$, we have

$$\frac{A_1 u_1 + (A_2 - A_1) u_2 + \ldots + (A_n - A_{n-1}) u_n}{A_n} \to 0,$$

and combining these relations we obtain

$$(2) \qquad \frac{A_1 u_1 + A_2 u_2 + \ldots + A_n u_n}{A_n} \to 0.$$

Now let $A_n = 1/a_n$, and we obtain

$$(3) \qquad (\epsilon_1 + \epsilon_2 + \ldots + \epsilon_n) a_n \to 0,$$

or

$$(3') \qquad (p_n - q_n) a_n \to 0.$$

If $na_n > K$, for $n > n_0$, it follows that

$$(4) \qquad (p_n - q_n)/n \to 0,$$

and the theorem is proved. It should be observed, however, that Cesàro has proved *more* than the theorem, the relation (3′) giving in general more information than (4).

3. The following proof of the theorem of § 2, though perhaps less elegant than Cesàro's, is in some ways more direct and even simpler.

We have*

(5) $$s_n = \sum_{1}^{n-1} (p_\nu - q_\nu)\,\Delta a_\nu + (p_n - q_n)\,a_n$$

and

(6) $$s_n - s_m = -(p_m - q_m)\,a_{m+1} + \sum_{m+1}^{n-1} (p_\nu - q_\nu)\,\Delta a_\nu + (p_n - q_n)\,a_n.$$

Suppose that, if possible, $(p_n - q_n)\,a_n$ has not the limit zero. Then we can find a positive number δ such that either

$$(p_n - q_n)\,a_n > \delta$$

for an infinity of values of n, or

$$(p_n - q_n)\,a_n < -\delta$$

for an infinity of values of n; let us say the former. Let $n_1, n_2, \ldots$ be such an infinity of values of n. Then, *unless $p_n - q_n$ is ultimately of constant sign*, we can associate with each n_i the greatest m_i for which $p_m - q_m \leqq 0$, and $m_i \to \infty$ with n_i. But then, from (6),

$$s_{n_i} - s_{m_i} > \delta,$$

which contradicts the hypothesis that s_n has a limit.

If, however, $p_n - q_n$ is ultimately of constant sign, let U, L be the maximum and minimum limits of $(p_n - q_n)\,a_n$, so that $0 \leqq L \leqq U$. Then we can find an infinity of values n_i such that

$$(p_n - q_n)\,a_n > U - \epsilon \quad (n = n_i),$$

and another of values m_i such that

$$(p_m - q_m)\,a_m < L + \epsilon \quad (m = m_i),$$

ϵ being an arbitrary positive number; and, from (6),

$$s_{n_i} - s_{m_i} > U - L - 2\epsilon,$$

for all pairs n_i, m_i such that $n_i > m_i$. And this again contradicts the hypothesis that s_n has a limit, unless $U = L$. There remains only the possibility that

$$(p_n - q_n)\,a_n \to l > 0.$$

---

* Bromwich, *Infinite Series*, p. 53.

But then it follows, from (5), that

$$\Sigma \frac{a_\nu - a_{\nu+1}}{a_\nu}$$

is convergent, and therefore that

$$\Pi \left(1 - \frac{a_\nu - a_{\nu+1}}{a_\nu}\right) = \Pi \left(\frac{a_{\nu+1}}{a_\nu}\right)$$

is convergent; and as $a_n \rightarrow 0$ this is untrue. Thus Cesàro's theorem is established. The proof just given has the advantage of proceeding directly from first principles.

4. The question also arises as to whether Cesàro's result fairly represents the *maximum* of information of this kind about $p_n - q_n$ that can be obtained from a knowledge of the convergence of $\Sigma (\pm a_n)$. The following examples indicate that this is, substantially, the case.

(i) Let $a_n = n^{-s}$, where $0 < s < 1$, and let us start from the convergent series

(7) $$1^{-s} - 2^{-s} + 3^{-s} - \dots .$$

Take a number t, greater than unity: it is convenient to suppose s and t *irrational.**

Of the two integers nearest to n^t, one less than and one greater than n^t, one is odd and one even. Let us denote the even one by $\phi(n)$. And now let us alter the series (7) by changing the sign of

$$u_{\phi(n)} \quad (n = 1, 2, \dots)$$

from *minus* to *plus*.† We thus obtain a series which is convergent or divergent according as

$$\Sigma \{\phi(n)\}^{-s}$$

is convergent or divergent: and it is easy to see that this series converges or diverges with Σn^{-st}; *i.e.*, converges if and only if

(8) $$t > 1/s.$$

* The purpose of this hypothesis is merely to avoid certain slight and entirely irrelevant complications, which do not make the least difference to the result.

† It may happen, for some of the first values of n, that successive values of $\phi(n)$ coincide. Thus, if $t = \frac{9}{8}$, $\phi(1) = \phi(2) = 2$. In what follows we ignore this possibility, which is plainly without effect on the result.

Now, if n is even, the value of $p_n - q_n$ is plainly $2m$, where m is determined by

$$\phi(m) \leqq n < \phi(m+1).$$

That is to say, $p_n - q_n$ is of order $n^{1/t}$, and the condition

$$(p_n - q_n)\, a_n \rightarrow 0$$

reduces to $$n^{-s+(1/t)} \rightarrow 0,$$

or $t > 1/s$. Comparing this result with (8) we see that the series converges or diverges according as Cesàro's condition is or is not satisfied.

(ii) Consider the series

$$(9) \qquad \Sigma(\pm n^{-s}) = \sum_{1^t}^{2^t-1} n^{-s} - \sum_{2^t}^{3^t-1} n^{-s} + \sum_{3^t}^{4^t-1} n^{-s} - \dots,$$

where $0 < s < 1$, and t is a positive integer greater than unity. The k^{th} group of terms is

$$(-1)^{k-1}\left\{\left(\sum_{1}^{(k+1)^t-1} - \sum_{1}^{k^t-1}\right) n^{-s}\right\},$$

and a little elementary calculation shows that the contents of the large bracket may be expressed in the form

$$tk^{(1-s)t-1} + R_k,$$

where the order of R_k, as a function of k, is that of $k^{(1-s)t-2}$. It follows that the series (9) is convergent if, and only if, $(1-s)\,t - 1 < 0$, *i.e.*, if $t < 1/(1-s)$.

Now, if $n = (2m)^t - 1$, it is clear that

$$p_n - q_n = (2^t - 1^t) - (3^t - 2^t) + \dots + \{(2m)^t - (2m-1)\}^t = \tfrac{1}{2}t(2m)^{t-1} + \dots,$$

as appears from a little easy calculation, the neglected terms being of order $t-2$. Similarly, if $n = (2m+1)^t - 1$, we find

$$p_n - q_n = -\tfrac{1}{2}t\,(2m)^{t-1} + \dots.$$

In other words, the oscillations of $p_n - q_n$ about zero are of order m^{t-1} or $n^{1-(1/t)}$; and Cesàro's condition is satisfied if, and only if,

$$n^{-s+1-(1/t)} \rightarrow 0,$$

or $t < 1/(1-s)$. In other words, the series converges or oscillates according as Cesàro's condition is or is not satisfied.

These two examples seem to show sufficiently clearly what is the answer to the question raised at the beginning of this section: it would not be difficult to formulate general theorems.

5. In Cesàro's equation (2) of § 2 we may, instead of putting $A_n = 1/a_n$, put $A_n = b_n/a_n$, where b_n is a function of n which tends to zero less rapidly than a_n. Then

$$\frac{\epsilon_1 b_1 + \epsilon_2 b_2 + \ldots + \epsilon_n b_n}{(b_n/a_n)} \to 0.$$

Thus the convergence of

$$\pm \frac{1}{1} \pm \frac{1}{2} \pm \ldots \ \ldots$$

involves the relation

$$\frac{1}{\sqrt{n}} \left(\pm \frac{1}{\sqrt{1}} \pm \frac{1}{\sqrt{2}} \pm \ldots \pm \frac{1}{\sqrt{n}} \right) \to 0.$$

This also enables us to obtain some information in the case in which $na_n \to 0$, when Cesàro's relation (3′) gives no information, $p_n - q_n$ being certainly less than n. For example, if we take $b_n = 1/n$, we obtain

$$na_n \{\epsilon_1 + \tfrac{1}{2}\epsilon_2 + \ldots + (1/n)\epsilon_n\} \to 0;$$

and if $$a_n > K/(n \log n),$$

we may replace a_n in this relation by $1/(n \log n)$, so obtaining

$$\{\epsilon_1 + \tfrac{1}{2}\epsilon_2 + \ldots + (1/n)\epsilon_n\}/\log n \to 0.$$

In other words, if $\Sigma(\pm a_n)$ is convergent and Σa_n diverges at least as rapidly as

$$\Sigma \frac{1}{n \log n},$$

the numbers $\epsilon_n = \pm 1$ have the mean value zero in the sense of M. Riesz;* just as, when the series Σa_n diverges at least as rapidly as $\Sigma(1/n)$, they must have the mean value zero in the ordinary sense.

---

* *Comptes Rendus*, July 5, 1909; see also *Proc. L.M.S.*, vol. viii., p. 301, *et seq.*

CAYLEY'S LINEAR RELATION BETWEEN MINORS OF A SPECIAL THREE-ROW ARRAY.

By *Thomas Muir, LL.D.*

1. The special three-row array in question is

$$\begin{array}{lllll} a_0 & a_1 & a_2 & \dots & a_{n-1} \quad a_0' \quad a_1' \quad \dots \quad a'_{n-2} \\ a_1 & a_2 & a_3 & \dots & a_n \quad\;\; a_1' \quad a_2' \quad \dots \quad a'_{n-1} \\ a_0' & a_1' & a_2' & \dots & a'_{n-1} \quad a_0'' \quad a_1'' \quad \dots \quad a''_{n-2}, \end{array}$$

there being $2n-1$ columns and $3n$ different elements; and, denoting the first n columns by $1, 2, 3, \dots, n$, the last $n-1$ columns by $(1), (2), (3), \dots, (n-1)$, and the determinant whose columns are the h^{th}, k^{th}, and l^{th} columns of the array by $\{h, k, l\}$, Cayley asserts that

$$a_0\mathrm{I} + a_1\mathrm{II} + a_{n-1}\mathrm{III} + a_n\mathrm{IV} = 0,$$

where

$$\mathrm{I} = \{n, n-1, (2)\} + \{n, n-2, (3)\} + \dots + \{n, 2, (n-1)\},$$

$$\mathrm{II} = -\{n, n-1, (1)\} - \{n, n-2, (2)\} - \dots - \{n, 2, (n-2)\} - \{n, 1, (n-1)\},$$

$$\mathrm{III} = -\{1, 2, (n-1)\} - \{1, 3, (n-2)\} - \dots - \{1, n-1, (2)\} - \{1, n, (1)\},$$

$$\mathrm{IV} = \{1, 2, (n-2)\} + \{1, 3, (n-3)\} + \dots + \{1, n-1, (1)\}.$$

For example, the array being

$$\begin{array}{llll} a & b & c & d \quad a' \quad b' \quad c' \\ b & c & d & e \quad b' \quad c' \quad d' \\ a' & b' & c' & d' \quad a'' \quad b'' \quad c'', \end{array}$$

the identity is

$$0 = a\begin{vmatrix} d & c & b' \\ e & d & c' \\ d' & c' & b'' \end{vmatrix} + a\begin{vmatrix} d & b & c' \\ e & c & d' \\ d' & b' & c'' \end{vmatrix} - b\begin{vmatrix} d & c & a' \\ e & d & b' \\ d' & c' & a'' \end{vmatrix} - b\begin{vmatrix} d & b & b' \\ e & c & c' \\ d' & b' & b'' \end{vmatrix} - b\begin{vmatrix} d & a & c' \\ e & b & d' \\ d' & a' & c'' \end{vmatrix}$$

$$+ e\begin{vmatrix} a & b & b' \\ b & c & c' \\ a' & b' & b'' \end{vmatrix} + e\begin{vmatrix} a & c & a' \\ b & d & b' \\ a' & c' & a'' \end{vmatrix} - d\begin{vmatrix} a & b & c' \\ b & c & d' \\ a' & b' & c'' \end{vmatrix} - d\begin{vmatrix} a & c & b' \\ b & d & c' \\ a' & c' & b'' \end{vmatrix} - d\begin{vmatrix} a & d & a' \\ b & e & b' \\ a' & d' & a'' \end{vmatrix}.$$

Strictly speaking, no proof is given of the truth of the general assertion, save that the cases for which n is 3, 4, 6 are established by a verificatory process. Unfortunately also this process is not at all concise or elegant or suggestive of generalization. It is accordingly now proposed to effect an improvement in all these respects.

2. Instead of discarding the use of determinants, as Cayley does, let us rather aim at condensation by employing determinants of the next higher order. The identity just written then becomes

$$0 = \begin{vmatrix} a & b & . & . \\ b & c & d & b' \\ c & d & e & c' \\ b' & c' & d' & b'' \end{vmatrix} + \begin{vmatrix} a & b & d & . \\ a & b & d & c' \\ b & c & e & d' \\ a' & b' & d' & c'' \end{vmatrix} - \begin{vmatrix} b & d & e & . \\ a & c & d & a' \\ b & d & e & b' \\ a' & c' & d' & a'' \end{vmatrix} - \begin{vmatrix} . & d & e & . \\ a & b & c & b' \\ b & c & d & c' \\ a' & b' & c' & b'' \end{vmatrix},$$

and it is established with ease by examining the co-factors of the elements in the last columns. (I.)

Further, we are led thus to see that its validity in no way depends on the fact that the variables a', b', c', d' in the third row of the array are the same as those in certain places of the two preceding rows. As a first generalization, consequently, we have the proposition that the identity holds in regard to the array

$$\begin{array}{cccc} a\ b\ c\ d & a' & b' & c' \\ b\ c\ d\ e & b' & c' & d' \\ \alpha\ \beta\ \gamma\ \delta & a'' & b'' & c''. \end{array} \qquad \text{(II.)}$$

Another fact less likely to be observed, but arising out of the same mode of verification, is that the d in the second row of this array need not be identical with the d of the first row, and that we may therefore replace it by D. Our extended result thus is

$$0 = \begin{vmatrix} a & b & . & . \\ b & c & d & b' \\ c & D & e & c' \\ \beta & \gamma & \delta & b'' \end{vmatrix} + \begin{vmatrix} a & b & d & . \\ a & b & d & c' \\ b & c & e & d' \\ \alpha & \beta & \delta & c'' \end{vmatrix} - \begin{vmatrix} b & D & e & . \\ a & c & d & a' \\ b & D & e & b' \\ \alpha & \gamma & \delta & a'' \end{vmatrix} - \begin{vmatrix} . & d & e & . \\ a & b & c & b' \\ b & c & D & c' \\ \alpha & \beta & \gamma & b'' \end{vmatrix},$$

(III.)

In the third place it is manifest that we may insert a new variable ω in the $(1,3)^{\text{th}}$ place of the first determinant provided we at the same time insert the same variable in the $(1,1)^{\text{th}}$ place of the fourth determinant. Fourthly, since by the deletion of the first row and last column of the four determinants we obtain the primary minors of the array

$$\begin{matrix} a & b & c & d \\ b & c & D & e \\ \alpha & \beta & \gamma & \delta, \end{matrix}$$

it follows that we may put a, c, b, d or b, D, c, e or $\alpha, \gamma, \beta, \delta$ in the $(1,4)^{\text{th}}$ places of the said determinants without destroying the identity. (IV.)

And lastly we may put $\theta_1, \theta_2, \theta_3, \theta_4$ in the said $(1,4)^{\text{th}}$ places provided the zero of the left-hand side of the identity be changed into

$$-\begin{vmatrix} \theta_1 & \theta_3 & \theta_2 & \theta_4 \\ a & b & c & d \\ b & c & D & e \\ \alpha & \beta & \gamma & \delta \end{vmatrix}.$$

Our final result thus is that *in regard to the twenty-two variables*

$$\begin{matrix} a & b & c & d & a' & b' & c' \\ b & c & D & e & b' & c' & d' \\ \alpha & \beta & \gamma & \delta & a'' & b'' & c'' \end{matrix} \qquad \begin{matrix} \omega \\ \theta_1 \; \theta_2 \; \theta_3 \; \theta_4 \end{matrix}$$

there exists the identity

$$\begin{vmatrix} a & b & d & \theta_1 \\ a & b & d & c' \\ b & c & e & d' \\ \alpha & \beta & \delta & c'' \end{vmatrix} + \begin{vmatrix} a & b & \omega & \theta_2 \\ b & c & d & b' \\ c & D & e & c' \\ \beta & \gamma & \delta & b'' \end{vmatrix}$$

$$- \begin{vmatrix} b & D & e & \theta_3 \\ a & c & d & a' \\ b & D & e & b' \\ \alpha & \gamma & \delta & a'' \end{vmatrix} - \begin{vmatrix} \omega & d & e & \theta_4 \\ a & b & c & b' \\ b & c & D & c' \\ \alpha & \beta & \gamma & b'' \end{vmatrix} = - \begin{vmatrix} \theta_2 & \theta_3 & \theta_1 & \theta_4 \\ a & b & c & d \\ b & c & D & e \\ \alpha & \beta & \gamma & \delta \end{vmatrix} \qquad \text{(V.)}$$

It may, evidently, also be viewed as an addition to the subject of *vanishing aggregates of four-line determinants.*

3. The same series of steps in generalization are possible in every case. Thus the first two steps give us, in reference to the array

$$\begin{array}{ccccc} a & b & e & h & m \quad p\ q\ s\ v \\ b & e & h & k & n \quad q\ s\ v\ y \\ c & f & i & l & o \quad r\ t\ w\ z, \end{array}$$

the identity

$$\begin{vmatrix} a & b & m & . \\ a & b & m & v \\ b & e & n & y \\ c & f & o & z \end{vmatrix} + \begin{vmatrix} a & b & . & . \\ b & e & m & s \\ e & h & n & v \\ f & i & o & w \end{vmatrix} + \begin{vmatrix} a & b & . & . \\ e & h & m & q \\ h & k & n & s \\ i & l & o & t \end{vmatrix}$$

$$- \begin{vmatrix} b & k & n & . \\ a & h & m & p \\ b & k & n & q \\ c & l & o & r \end{vmatrix} - \begin{vmatrix} . & m & n & . \\ a & e & h & q \\ b & h & k & s \\ c & i & l & t \end{vmatrix} - \begin{vmatrix} . & m & n & . \\ a & b & e & s \\ b & e & h & v \\ c & f & i & w \end{vmatrix} = 0, \qquad \text{(VI.)}$$

which degenerates into Cayley's when special values are given to k, c, f, i, l, o. If, further, we fill the vacant places of the determinants by the elements

$$\theta_1,\ \omega_1,\ \theta_2,\ \omega_2,\ \theta_3,\ \theta_6,\ \omega_2,\ \theta_5,\ \omega_1,\ \theta_4$$

in order, and change the 0 on the right-hand side into

$$- \begin{vmatrix} \theta_2 & \xi & \theta_1 & \theta_4 \\ a & b & e & m \\ b & e & h & n \\ c & f & i & o \end{vmatrix} - \begin{vmatrix} \theta_3 & \theta_6 & \xi & \theta_5 \\ a & e & h & m \\ b & h & k & n \\ c & i & l & o \end{vmatrix},$$

an identity still subsists. (VII.)

4. When the number of columns of the given array is $n+(n-1)$, the number of variables in the generalized result is $8n-10$, the number of determinants on the left of the identity is $2n-4$, and on the right $n-3$. (VIII.)

The determinants on the left have three columns taken from the first part of the array and one from the second part: they are best written in two rows because of the correspondence due to a partial reversibility. The determinants on the right have four columns taken from the first part of the array and none from the second.

5. In establishing (VI.) in the manner mentioned in § 2 we find the vanishing co-factors in the case of y, z, p, r to be one determinant, in the case of w, t to be an aggregate of two determinants, in the case of v, q to be an aggregate of three determinants, and in the case of s to be an aggregate of four determinants. It is only the last case that presents anything fresh, the identity being

$$\begin{vmatrix} a & b & \theta_1 \\ e & h & m \\ f & i & o \end{vmatrix} - \begin{vmatrix} a & b & \theta_2 \\ e & h & m \\ i & l & o \end{vmatrix} + \begin{vmatrix} \theta_2 & m & n \\ a & e & h \\ c & i & l \end{vmatrix} - \begin{vmatrix} \theta_1 & m & n \\ b & e & h \\ c & f & i \end{vmatrix} = 0. \qquad \text{(IX.)}$$

In this there are thirteen variables, of which six occur twice, four three times, and three four times. It is thus distinct from Kronecker's outwardly similar result, which has fourteen variables, of which six occur twice and eight three times. It is most readily established by noting that θ_1, θ_2, o, c having vanishing co-factors may be deleted, and that what then remains may be written

$$\begin{vmatrix} a & b & . \\ i & l & n \\ f & i & m \end{vmatrix} + \begin{vmatrix} . & m & n \\ a & f & i \\ b & i & l \end{vmatrix},$$

which evidently vanishes.

6. Kronecker's theorem just referred to has unfortunately always been looked upon as predicating the vanishing of an aggregate of n-line minors of a $2n$-line axisymmetric determinant, its author having originally arrived at it in this connection. The following is a much more useful way of looking at the fundamental result: *If an array of n rows and $2n-2$ columns have its first principal minor symmetric with respect to a zero diagonal, the aggregate of the $(n-1)$-line minors which are free of zero elements vanishes.* (X.)

Thus, when n is 4, such an array is

$$\begin{matrix} . & a & b & c & \alpha_1 & \alpha_2 \\ a & . & d & e & \beta_1 & \beta_2 \\ b & d & . & f & \gamma_1 & \gamma_2 \\ c & e & f & . & \delta_1 & \delta_2, \end{matrix}$$

and we have

$$\begin{vmatrix} a & \beta_1 & \beta_2 \\ b & \gamma_1 & \gamma_2 \\ c & \delta_1 & \delta_2 \end{vmatrix} - \begin{vmatrix} a & \alpha_1 & \alpha_2 \\ d & \gamma_1 & \gamma_2 \\ e & \delta_1 & \delta_2 \end{vmatrix} + \begin{vmatrix} b & \alpha_1 & \alpha_2 \\ d & \beta_1 & \beta_2 \\ f & \delta_1 & \delta_2 \end{vmatrix} - \begin{vmatrix} c & \alpha_1 & \alpha_2 \\ e & \beta_1 & \beta_2 \\ f & \gamma_1 & \gamma_2 \end{vmatrix} = 0.$$

Proof is obtained at once by examining the co-factors of the elements of the four first columns.

Cape Town, S.A.,
January 25th, 1911.

NUMBER OF THE ABELIAN SUB-GROUPS IN THE POSSIBLE GROUPS OF ORDER 2^m.

By *G. A. Miller*.

THE theorem that every group G of order p^m, p being an arbitrary prime number, contains an abelian sub-group of order p^a whenever

$$m > \tfrac{1}{2}\alpha(\alpha-1)$$

was proved in this Journal, vol. xxvii. (1897–98), p. 120. In a later number of the same Journal, vol. xxxvi. (1906–7), p. 79, it was observed that the given theorem can be stated more completely by adding that G must contain an *invariant* abelian sub-group of order p^a whenever

$$m > \tfrac{1}{2}\alpha(\alpha-1).$$

Moreover, it was observed in this later article that in the very special case when $p=2$ and $\alpha=4$ it is possible to extend the theorem, since every group of order 64 contains an abelian invariant sub-group of order 16. In the present article we shall prove that the theorem in question can be extended for all values of $\alpha>3$, when $p=2$. We shall also establish a useful theorem as regards the number of the abelian sub-groups in any group of order p^m.

In the former of the two articles mentioned above it was proved that G involves a sub-group K of order

$$p^{m-1-2-\ldots-(\beta-3)} = p^{m-\frac{1}{2}\{(\beta-2)(\beta-3)\}},$$

whose central* is at least of order $p^{\beta-2}$, $\beta>3$, whenever

$$m \geqq \tfrac{1}{2}\{(\beta-1)(\beta-2)\}.$$

* The central of a group is composed of the totality of the invariant operators of the group.

When $m = \frac{1}{2}\beta(\beta - 1)$ the order of K is $p^{2\beta-3}$, and its quotient group, with respect to the given central C, is of order $p^{\beta-1}$. If this quotient group contains operators of order p^2, G evidently contains an abelian sub-group of order p^β, and the theorem mentioned above has been extended. It remains therefore to consider the case when this quotient group does not involve any operator of order p^2, and hence we may assume that it is abelian when $p = 2$. In what follows we shall confine our attention to this special case.

We are thus led to consider the possibility of constructing a group K of order $2^{2\beta-3}$, having a central C of order $2^{\beta-2}$ which gives rise to an abelian quotient group of type $(1, 1, \ldots)$. If we arrive at a contradiction by assuming that K does not include an abelian sub-group of order 2^β, the extension in question will have been effected. If K would not include an abelian sub-group of order 2^β all the operators of C, excepting identity, would be of order 2, since all these operators would be commutators and the commutator quotient group would not involve any operator of order 4. Hence the order of each of the operators of G would divide 4 Moreover, each of the non-invariant operators of K would be transformed under K into itself multiplied by all the operators of C.

Let K_1 represent any sub-group of order $2^{2\beta-4}$ which is in K and includes C. Each of the non-invariant operators of K_1 is transformed under K_1 into itself multiplied by all the operators of a sub-group of order $2^{\beta-3}$ contained in C. The multiplying sub-groups of order $2^{\beta-3}$ for two distinct $(\bmod C)$ operators of K_1 must be distinct, otherwise the operators of the group of order 4 $(\bmod C)$ generated by these two operators would have to be transformed by an operator of K which is not also in K_1 into themselves multiplied by the operators of a group of order 4 which would have only the identity in common with the given sub-group of order $2^{\beta-3}$ in C. As such a group of order 4 can clearly not exist in C it results that all the different $(\bmod C)$ non-invariant operators of K_1 are transformed under K_1 into themselves multiplied by all the different sub-groups of order $2^{\beta-3}$ in C.

From the preceding it results that there is a $(1, 1)$ correspondence between the operators of K_1 and the sub-groups of order $2^{\beta-3}$ in C such that each operator of K_1 is transformed under K_1 into itself multiplied by the various operators of the corresponding sub-group. Let t_1 be any non-invariant operator of K_1, and consider all the possible sub-groups of order 4 $(\bmod C)$ such that each of these sub-groups involves t_1. Any operator ρ of K which is not also in K_1 transforms each

of these sub-groups into itself multiplied by a sub-group of order 4 in C. Let $t_1, t_2, \ldots, t_{\beta-2}$ be a set of operators of K_1 which have a (1,1) correspondence with a set of independent generators in the quotient group of K_1 with respect to C, and assume that

$$t_1^{-1}t_2t_1 = s_1t_2,\ t_1^{-1}t_3t_1 = s_2t_3,\ \ldots,\ t_1^{-1}t_{\beta-2}t_1 = s_{\beta-3}t_{\beta-2}.$$

The sub-group (t_1, t_2) is transformed by ρ into itself multiplied by a group of order 4 which does not involve s_1. In general, the sub-group (t_1, t_α), $\alpha = 2, 3, \ldots, \beta - 2$, is transformed by ρ into itself multiplied by a sub-group of order 4 in C which does not involve $s_{\alpha-1}$, and the sub-group $t_1, t_{\alpha_1}t_{\alpha_2}\ldots t_{\alpha_\lambda}$ is transformed by ρ into itself multiplied by a sub-group of C which does not involve $s_{\alpha_1-1}s_{\alpha_2-1}\ldots s_{\alpha_\lambda-1}$ $(\alpha_1, \alpha_2, \ldots \alpha_\lambda = 1, 2, \ldots, \beta - 2)$. As ρ must transform t_1 into itself multiplied by an operator of C which is common to all of these sub-groups of order 4 and as $s_1, s_2, \ldots, s_{\beta-3}$ is a set of independent generators of a sub-group of order $2^{\beta-3}$ contained in C, it results that the commutator of t_1, ρ appears in a sub-group of order 4 which does not exist. That is, we have arrived at a contradiction by assuming that K does not involve an abelian sub-group of order 2^β, and hence we have proved that *every group of order* 2^m *contains an abelian sub-group of order* 2^β *provided* $m \geqq \frac{1}{2}\beta(\beta - 1)$.

It remains to prove that at least one of these abelian sub-groups of order 2^β is invariant under G. This will evidently follow from the theorem stated at the end of the preceding paragraph provided we can show that the number of abelian sub-groups of any order in a group of order 2^m is either 0 or an odd number. This, in turn, is included in the more general theorem that the number of abelian sub-groups of order p^a in any group G of order p^m is either 0 or of the form $kp + 1$. We proceed to prove this theorem. It is known that the number of abelian sub-groups of order p^a, which involve a given group of order p^{a-1}, is of the form $1 + kp$ whenever it is not 0,* and that the number of sub-groups of order p^{a-1} in any group of order p^a is of the form $1 + kp$.

In the group G, which involves at least one abelian sub-group of order p^a, let r_x represent the number of the abelian sub-groups of order p^a in which a given abelian group of order p^{a-1} occurs, while r_y represents the number of the sub-groups of order p^{a-1} in a given abelian sub-group of order p^a. It was observed above that $r_x \equiv 1 \pmod{p}$ and $r_y \equiv 1$

* *Messenger of Mathematics*, vol. xxxvi. (1906–7), p. 79.

(mod p). If we represent the total number of distinct abelian sub-groups of orders $p^{\alpha-1}$ and p^{α} in G by $r_{\alpha-1}$ and r_{α} respectively, we have the equation

$$\sum_{x=1}^{x=r_{\alpha-1}} r_x = \sum_{y=1}^{y=r_{\alpha}} r_y.$$

Each member of this equation represents the sum obtained by counting every abelian sub-group of order p^{α} as many times as it contains sub-groups of order $p^{\alpha-1}$. Hence $r_{\alpha} \equiv r_{\alpha-1}$ (mod p). Since $r_{\alpha-1} \equiv 1$ (mod p), when $\alpha = 2$, we have proved the theorem: *The number of the abelian sub-groups of order p^{α} in any group of order p^m is of the form $kp+1$ whenever this number is not zero.* As a corollary of this theorem and the one proved above we have that *every group of order 2^m contains an invariant abelian sub-group of order 2^{β} whenever*

$$m \geqq \tfrac{1}{2}\beta(\beta-1).$$

PROOF OF AN INEQUALITY.

By *R. S. Heath*, late Fellow of Trinity College, Cambridge; Vice-Principal of the University of Birmingham.

In his *Algebra*, chap. xxiv., §7, Professor Chrystal enunciates and proves the following inequalities: *If x and y be positive and unequal, then*

$$mx^{m-1}(x-y) > x^m - y^m > my^{m-1}(x-y)$$

unless $0 < m < 1$, in which case the inequalities are reversed.

Let a and b be positive numbers and $a > b$, and let p be any positive integer. Consider the geometrical progression containing the following terms:

$$\ldots,\ a^{p-1},\ a^{p-2}b,\ a^{p-3}b^2,\ \ldots,\ ab^{p-2},\ b^{p-1},\ \ldots\ .$$

The average of the terms written down is

$$\frac{1}{p}\,\frac{a^p-b^p}{a-b}.$$

Now, if q be any positive integer $<p$, the average of these terms is less than the average of q terms commencing with a^{p-1} and is greater than the average of q terms ending with b^{p-1}, but if $q>p$ these inequalities are reversed. Thus, if $q<p$,

$$a^{p-q}\,\frac{1}{q}\,\frac{a^q-b^q}{a-b} > \frac{1}{p}\,\frac{a^p-b^p}{a-b} > b^{p-q}\,\frac{1}{q}\,\frac{a^q-b^q}{a-b}.$$

If q be a negative integer, the inequalities are still stronger. For let $q=-k$. Then the average of the k terms, immediately preceding a^{p-1}, is

$$\frac{a^p}{b^k}\frac{1}{k}\frac{a^k-b^k}{a-b}=a^{p+k}\frac{1}{k}\frac{b^{-k}-a^{-k}}{a-b}$$
$$=a^{p-q}\frac{1}{q}\frac{a^q-b^q}{a-b}.$$

Similarly the average of the k terms, immediately following the term b^{p-1}, is

$$b^{p-q}\frac{1}{q}\frac{a^q-b^q}{a-b}.$$

Multiplying up by $p(a-b)$, which is positive, we get the following result:

If q be any negative or positive integer $<p$,

$$\frac{p}{q}a^{p-q}(a^q-b^q)>a^p-b^p>\frac{p}{q}b^{p-q}(a^q-b^q);$$

but if $q>p$ these inequalities are reversed.

The inequalities are strongest when q is negative and numerically large; as q increases up to p, the inequalities get weaker and weaker until, when $q=p$, they become equalities. When q increases from p onwards the inequalities are reversed and are at first weak, but get stronger and stronger.

The condition that $a>b$ can be removed. For if $b>a$ the same theorem shows that if $q<p$

$$\frac{p}{q}b^{p-q}(b^q-a^q)>b^p-a^p>\frac{p}{q}a^{p-q}(b^q-a^q),$$

and therefore, changing signs, we get the same result as before.

Let $$a^q=x,\quad b^q=y,\quad \frac{p}{q}=m.$$

Then $mx^{m-1}(x-y)>x^m-y^m>my^{m-1}(x-y)$ for all values of m (except 0), with the reservation that if $0<m<1$, the inequalities are reversed.

When $m=1$ the inequalities become equalities. As m increases from 1 to M and then through the negative values from $-M$ to $-\epsilon$ the inequalities get stronger and stronger, M being any positive number, however large, and ϵ any positive number, however small; as m diminishes from 1 to ϵ the reversed inequalities get stronger and stronger.

BIBLIOGRAPHY OF KIRKMAN'S SCHOOLGIRL PROBLEM.

By *Oscar Eckenstein.*

A.—Papers.

1. T. P. Kirkman, "On a problem in combinations," *Cambridge and Dublin Mathematical Journal*, vol. ii. (1847), pp. 191–204.

2. T. P. Kirkman, "Query," *Lady's and Gentleman's Diary* (1850), p. 48.

3. A. Cayley, "On the triadic arrangements of seven and fifteen things," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. xxxvii. (1850), pp. 50–53.

4. T. P. Kirkman, "Note on an unanswered prize question," *Cambridge and Dublin Mathematical Journal*, vol. v. (1850), pp. 255–262.

5. T. P. Kirkman, "On the triads made with fifteen things," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. xxxvii. (1850), pp. 169–171.

6. "Solutions to Query VI," *Lady's and Gentleman's Diary* (1851), p. 48.

7. R. R. Anstice, "On a problem in combinations," *Cambridge and Dublin Mathematical Journal*, vol. vii. (1852), pp. 279–292.

8. R. R. Anstice, "On a problem in combinations" (continued from vol. vii., p. 292), *Cambridge and Dublin Mathematical Journal*, vol. viii. (1853), pp. 149–154.

9. J. Steiner, "Combinatorische Aufgabe," *Crelle's Journal für die reine und angewandte Mathematik*, vol. xlv. (1853), pp. 181–182.

10. T. P. Kirkman, "Theorems on combinations," *Cambridge and Dublin Mathematical Journal*, vol. viii. (1853), pp. 38–45.

11. T. P. Kirkman, "On the perfect r partitions of $r^2 - r + 1$," *Transactions of the Historic Society of Lancashire and Cheshire*, vol. ix. (1856–1857), pp. 127–142.

12. B. Peirce, "Cyclic solutions of the school-girl puzzle," *Astronomical Journal* (U.S.A.), vol. vi. (1860), pp. 169–174.

13. J. J. Sylvester, "Note on the historical origin of the unsymmetrical six-valued function of six letters," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. xxi. (1861), ser. 4, pp. 369–377.

14. W. S. B. Woolhouse, "On the Rev. T. P. Kirkman's problem respecting certain triadic arrangements of fifteen symbols," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. xxi. (1861), pp. 510–515.

15. J. J. Sylvester, "On a problem in tactic which serves to disclose the existence of a four-valued function of three sets of three letters each," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. xxi. (1861), ser. 4, pp. 515–520.

16. W. S. B. Woolhouse, "On triadic combinations of 15 symbols," *Lady's and Gentleman*'s *Diary* (1862), pp. 84-88.

17. Paper No. 16 is reprinted in the *Assurance Magazine*, vol. x. (1862), pt. v., No. 49, pp. 275–281.

18. T. P. Kirkman, "On the puzzle of the fifteen young ladies," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. xxiii. (1862), ser. 4, pp. 198–204.

19. A. Cayley, "On a tactical theorem relating to the triads of fifteen things," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. xxv. (1863), ser. 4, pp. 59–61.

20. W. S. B. Woolhouse, "On triadic combinations," *Lady's and Gentleman's Diary* (1863), pp. 79–90.

21. J. Power, "On the problem of the fifteen school-girls," *Quarterly Journal of Pure and Applied Mathematics*, vol. viii. (1867), pp. 236–251.

22. S. Bills, "Solution of problem proposed by W. Lea," *Educational Times Reprints*, vol. viii. (1867), pp. 32–33.

23. W. Lea, "Solution of problem proposed by himself," *Educational Times Reprints*, vol. ix. (1868), pp. 35–36.

24. T. P. Kirkman, "Solution of three problems proposed by W. Lea," *Educational Times Reprints*, vol. xi. (1869), pp. 97–99.

25. A. Frost, "General solution and extension of the problem of the fifteen schoolgirls," *Quarterly Journal of Pure and Applied Mathematics*, vol. xi. (1871), pp. 26–37.

26. W. Lea, "Solution of problem proposed by himself," *Educational Times Reprints*, vol. xxii. (1874), pp. 74–76.

27. J. J. Sylvester, "Proposed problem," *Educational Times*, November 1, 1875, p. 193.

28. Appendix note, *Proceedings of the London Mathematical Society*, vol. vii. (1875), pp. 235–237.

29. E. Carpmael, "Some solutions of Kirkman's 15-school-girl problem," *Proceedings of the London Mathematical Society*, vol. xii. (1881), pp. 148–156.

30. "A fifteen puzzle," *Knowledge*, vol. i. (1881), p. 80.

31. A. Bray, "The fifteen schoolgirls," *Knowledge*, vol. ii. (1882), pp. 80–81.

32. E. Marsden, "The school-girls' problem," *Knowledge*, vol. iii. (1883), p. 183.

33. A. Bray, "Twenty-one school-girl puzzle," *Knowledge*, vol. iii. (1883), p. 268.

34. J. J. Sylvester, "Note on a nine schoolgirls problem," *Messenger of Mathematics*, vol. xxii. (1893), pp. 159–160.

35. "Correction to the note on the nine schoolsgirls problem," *Messenger of Mathematics*, vol. xxii. (1893), p. 192.

36. A. C. Dixon, "Note on Kirkman's problem," *Messenger of Mathematics*, vol. xxiii. (1893), pp. 88–89.

37. W. Burnside, "On an application of the theory of groups to Kirkman's problem," *Messenger of Mathematics*, vol. xxiii. (1894), pp. 137–143.

38. E. H. Moore, "Tactical memoranda," *American Journal of Mathematics*, vol. xviii. (1896), pp. 264–303.

39. E. W. Davis, "A geometric picture of the fifteen school-girl problem," *Annals of Mathematics* (U.S.A.), vol. ii. (1896–1897), pp. 156–157.

40. A. F. H. Mertelsmann, "Das Problem der 15 Pensionatsdamen," *Zeitschrift für Mathematik und Physik*, vol. xliii. (1898), pp. 329–334.

41. W. Ahrens, "Review of Schubert's Mathematische Mussestunden," *Zeitschrift für mathematischen und naturwissenschaftlichen Unterricht*, vol. xxxi. (1900), pp. 386–388.

42. H. E. Dudeney, "Solution," *Educational Times Reprints*, vol. xiv. (1908), pp. 97–99.

43. H. E. Dudeney, "Solution" (continued), *Educational Times Reprints*, vol. xv. (1909), pp. 17–19.

44. O. Eckenstein, "Note," *Educational Times Reprints*, vol. xvi. (1909), pp. 76–77.

45. H. E. Dudeney, "Solution" (continued), *Educational Times Reprints*, vol. xvii. (1910), pp. 35–38.

46. O. Eckenstein, "Solutions," *Educational Times Reprints*, vol. xvii. (1910), pp. 38–39.

47. O. Eckenstein, "Note," *Educational Times Reprints*, vol. xvii. (1910), pp. 49–53.

48. W. W. Rouse Ball, "Proposed problem," *Educational Times* (February, 1, 1911), p. 82.

B.—Books dealing with the subject.

Nos. 4 and 5 contain some original matter, not previously published.

1. W. W. Rouse Ball, *Mathematical Recreations*, first edition, 1892, pp. 89–94.

2. Ditto, second edition, 1892, pp. 89–94.

3. Ditto, third edition, 1896, pp. 110–116.

4. Ditto, fourth edition, 1905, pp. 121–128.

5. E. Lucas, *Recréations Mathématiques*, first edition, 1891, vol ii., pp. 161–197.

6. Ditto, second edition, 1896, vol. ii., pp. 161–197.

7. H. Schubert, *Zwölf Geduldspiele*, new edition, 1899, pp. 20–25.

8. H. Schubert, *Mathematische Mussestunden*, second edition, 1900, vol. ii., pp. 49–66.

9. Ditto, third edition, 1909, vol. ii., pp. 49–66.

10. W. Ahrens, *Mathematische Unterhaltungen und Spiele*, 1901, pp. 257–285.

ON THE CONVERGENCE OF THE SERIES $\Sigma \frac{1}{(m_1^2+m_2^2+\ldots+m_r^2)^\mu}$.

By *F. Jackson, B.Sc.*, University College, London.

THE convergence of the series

$$\Sigma \frac{1}{(m_1^2+m_2^2+\ldots+m_r^2)^\mu},$$

where $m_1, m_2, \ldots, m_r$ may have all integral values from $-\infty$ to $+\infty$ (excepting the set of values where $m_1=m_2=\ldots=m_r=0$), can be investigated in the following remarkably easy manner.

[The original investigation was by Eisenstein, *Crelle's Journal*, xxxv., pp. 157–159.]

Let $u_n=$ the sum of all the terms of the series which satisfy the conditions:

(i) Every m numerically $\leqq n$.

(ii) *At least one* $m=\pm n$.

The series thus reduces to

$$u_1+u_2+\ldots+u_n+\ldots.$$

Consider the number of terms in

$$u_1+u_2+\ldots+u_n.$$

It is the same as the number of permutations of the $2n+1$ numbers

$$-n, -(n-1), -(n-2), \ldots, -1, 0, 1, \ldots, n-1, n,$$

taken r at a time, when each number may be repeated any number of times, the case, where $m_1=m_2=\ldots=m_r=0$, being excluded.

Therefore the number of terms is $(2n+1)^r-1$.

Therefore the number of terms making up u_n is

$$[(2n+1)^r-1]-[(2n-1)^r-1]$$

$$=(2n+1)^r-(2n-1)^r$$

$$=2\left(r 2^{r-1}n^{r-1}+{}_rC_3 2^{r-3}n^{r-3}+\ldots\begin{cases}+r.2.n & \text{if } r \text{ even}\\ +\quad 1 & \text{if } r \text{ odd}\end{cases}\right)$$

$$=An^{r-1}+Bn^{r-3}+\text{a finite number of lower powers of } n.$$

The coefficients A, B, &c., are constant and positive.

Now the greatest term in u_n (all the terms are positive) is

$$\frac{1}{n^{2\mu}},$$

the case where one $|m| = n$ and all other m's $= 0$.

Therefore

$$u_n < \frac{An^{r-1} + Bn^{r-3} + \text{lower powers of } n}{n^{2\mu}}.$$

Therefore Σu_n is convergent if $\Sigma \frac{n^{r-1}}{n^{2\mu}}$ is convergent. This latter series is absolutely convergent if

$$2\mu - (r-1) > 1, \text{ i.e., if } 2\mu > r.$$

Therefore the series $\Sigma \frac{1}{(m_1^2 + m_2^2 + \ldots + m_r^2)^\mu}$ is absolutely convergent if $2\mu > r$. Also the series is divergent if $2\mu \overline{\lessgtr} r$. For the least term in u_n is

$$\frac{1}{(rn^2)^\mu}.$$

Therefore

$$u_n > \frac{An^{r-1} + Bn^{r-3} + \ldots \text{ a finite number of terms}}{r^\mu n^{2\mu}},$$

where A, B, and all the other coefficients are positive. Therefore Σu_n is divergent if $\Sigma \frac{n^{r-1}}{n^{2\mu}}$ is divergent, which is the case if $2\mu - r + 1 \overline{\lessgtr} 1$, *i.e.*, if $2\mu \leq r$.

In a similar way it can be shown that the series

$$\Sigma \frac{1}{(m_1^\nu + m_2^\nu + \ldots + m_r^\nu)^\mu}$$

is convergent, if $\nu\mu > r$, and divergent, if $\nu\mu \leq r$, when ν is a positive even integer. But if ν is a positive odd integer, then we must restrict the m's to be positive integers.

NOTE ON A SPECIAL FORM OF TAYLOR'S REMAINDER AND ITS APPLICATION TO THE SERIES FOR $(1-2x\cos\alpha+x^2)^{-\frac{1}{2}}$ WHEN $|x|=1$.

By *L. N. G. Filon, M.A., D.Sc., F.R.S.*,
Assistant Professor of Mathematics at University College, London.

1. A GENERAL form of remainder after n terms in Taylor's series may be obtained as follows:

Let $f(z)$ be a function such that $f^{n-1}(z)$ is continuous between $z=x$ and $z=X$ inclusive, and $f^n(z)$ exists and is determinate between $z=x$ and $z=X$ exclusive.

Let R_n be the difference between $f(X)$ and the first n terms of its expansion in powers of $X-x$.

Let the function $F(z)$ be defined by the equation

$$F(z) \equiv f(X) - f(z) - (X-z)f'(z) - \ldots - \frac{(X-z)^{n-1}}{(n-1)!} f^{n-1}(z) \ldots (1).$$

Then $\qquad F(X)=0, \qquad F(x)=R_n.$

Consider $\qquad \phi(z)=F(z)-R_n\psi(z),$

where $\qquad \psi(X)=0, \qquad \psi(x)=1.$

Then $\qquad \phi(X)=0, \qquad \phi(x)=0.$

Now $\qquad F'(z)=-\dfrac{(X-z)^{n-1}}{(n-1)!}f^n(z).$

Hence, by the conditions satisfied by $f(z)$, we can apply the Theorem of the Mean Value to $\phi(z)$ provided $\psi(z)$ is continuous between $z=x$ and $z=X$ inclusive, and $\psi'(x)$ is determinate between $z=x$ and $z=X$ exclusive.

To avoid indeterminacy of $\phi'(z)$ through the subtraction of infinities, we shall suppose that the infinities of $\psi'(z)$ are different from those of $f_n(z)$.

Hence, for $z=x+\theta(X-x)$, where $0<\theta<1$,

$$F'\{x+\theta(X-x)\} - R_n\psi'\{x+\theta(X-x)\} = 0 \ldots (2).$$

If now we make the further supposition that $\psi'(z) \neq 0$ *between* $z = x$ and $z = X$, we may divide equation (2) by $\psi'\{x + \theta(X - x)\}$, and we find

$$R_n = -\frac{(X-x)^{n-1}(1-\theta)^{n-1} f^n\{x+\theta(X-x)\}}{(n-1)!\,\psi'\{x+\theta(X-x)\}} \quad \ldots(3).$$

2. If in (3) we put $\psi(z) = \dfrac{X-z}{X-x}$, we get Cauchy's form of the remainder. If we put $\psi(z) = \left(\dfrac{X-z}{X-x}\right)^n$, we get Lagrange's form. Schlömilch (*Höhere Analyse*) has shown that the remainder in the series for $\arcsin x$, when x is numerically equal to 1, can be obtained from a form of remainder which can be derived from (3) by taking

$$\psi(z) = \left(\frac{X-z}{X-x}\right)^{\frac{1}{2}}.$$

In what follows I propose to consider a somewhat different special form and to show how, by means of it, the remainder in the series for $(1 - 2x\cos\alpha + x^2)^{-\frac{1}{2}}$ can be dealt with when x is numerically equal to 1.

3. This new form of remainder is obtained as follows:

Take $$\psi(z) = \left(\frac{X-z}{X-x}\right)\left(1 - a\frac{z-x}{X-x}\right)^n,$$

where a is a positive constant lying between 0 and 1. It is immediately verified that this satisfies all the conditions laid down for $\psi(z)$.

It follows easily from (3) that

$$R_n = \frac{(X-x)^n(1-\theta)^{n-1} f^n\{x+\theta(X-x)\}}{(n-1)!\,[(1-a\theta)^n + na(1-\theta)(1-a\theta)^{n-1}]}.$$

Hence $$|R_n| < \frac{|X-x|^n(1-\theta)^{n-1}\,|f^n\{x+\theta(X-x)\}|}{(n-1)!\,na(1-\theta)(1-a\theta)^{n-1}},$$

$$< \frac{|X-x|^n}{n!\,a(1-a)}\left(\frac{1-\theta}{1-a\theta}\right)^{n-2} |f^n\{x+\theta(X-x)\}|$$

$$< \frac{|X-x|^n}{n!\,a(1-a)}\{1-(1-a)\theta\}^{n-2}|f^n\{x+\theta(X-x)\}|,$$

or, writing $1-a=b$,

$$|R_n| < \frac{|X-x|^n}{n!\,b(1-b)}(1-b\theta)^{n-2}|f^n\{x+\theta(X-x)\}|\ldots(4),$$

where $0<b<1$.

4. Now consider

$$y=(1-2x\cos\alpha+x^2)^{-\frac{1}{2}},$$

$$\frac{d^ny}{dx^n}=\frac{d^n}{dx^n}(e^{i\alpha}-x)^{-\frac{1}{2}}(e^{-i\alpha}-x)^{-\frac{1}{2}}$$

$$=\sum_{r=0}^{r=n}{}_nC_r\frac{d^r}{dx^r}(e^{i\alpha}-x)^{-\frac{1}{2}}\frac{d^{n-r}}{dx^{n-r}}(e^{-i\alpha}-x)^{-\frac{1}{2}}$$

$$=n!\sum_{r=0}^{r=n}\frac{(-\frac{1}{2})_r(-\frac{1}{2})_{n-r}}{r!\,(n-r)!}(-1)^n(e^{i\alpha}-x)^{-\frac{1}{2}-r}(e^{-i\alpha}-x)^{-\frac{1}{2}-n+r}$$

$$=n!\,(1-2x\cos\alpha+x^2)^{-\frac{1}{2}(n+1)}(-1)^n\sum_{r=0}^{r=n}\frac{(-\frac{1}{2})_r(-\frac{1}{2})_{n-r}}{r!\,(n-r)!}\left(\frac{e^{i\alpha}-x}{e^{-i\alpha}-x}\right)^{\frac{1}{2}n-r},$$

where $a_r=a(a-1)\ldots(a-r+1)$ and $a_0=1$. If $x=0$,

$$\left[\frac{d^ny}{dx^n}\right]_{x=0}=(-1)^n\,n!\sum_{r=0}^{r=n}\frac{(-\frac{1}{2})_r(-\frac{1}{2})_{n-r}}{r!\,(n-r)!}e^{2i\alpha(\frac{1}{2}n-r)}=n!\,P_n(\cos\alpha).$$

If $x\neq 0$, put

$$e^{i\alpha}-x=R\cos\phi+iR\sin\phi,$$

Then
$$e^{-i\alpha}-x=R\cos\phi-iR\sin\phi,$$

where
$$\tan\phi=\frac{\sin\alpha}{\cos\alpha-x}\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5),$$

and we have

$$\frac{d^ny}{dx^n}=n!\,(1-2x\cos\alpha+x^2)^{-\frac{1}{2}(n+1)}P_n(\cos\phi)\ldots\ldots(6).$$

Note that whatever value we give to x, other than infinity, ϕ differs from 0 or π by a finite amount, provided that α differs from 0 or π by a finite amount.

5. Now use the form of remainder (4), putting

$$f(z) = (1 - 2z\cos\alpha + z^2)^{-\frac{1}{2}},$$

and $x = 0$. We have

$$|R_n| < \frac{|X|^n}{b(1-b)} \frac{(1-b\theta)^{n-2}}{(1 - 2\theta X\cos\alpha + \theta^2 X^2)^{\frac{1}{2}(n+1)}} |P_n(\cos\phi)|.$$

But $$\frac{1-b\theta}{(1-2\theta X\cos\alpha + \theta^2 X^2)^{\frac{1}{2}}} < \frac{1-b\theta}{1-\theta\,|X\cos\alpha|} < 1,$$

provided $b > |X\cos\alpha|$, and this is always possible, even if $|X| = 1$, so long as α differs finitely from 0 or π. Thus

$$|R_n| < \frac{|X|^n}{b(1-b)(1-2\theta X\cos\alpha + \theta^2 X^2\cos^2\alpha)^{\frac{3}{2}}} |P_n(\cos\phi)|$$

$$< \frac{|X|^n}{b(1-b)(1-|X\cos\alpha|)^3} |P_n(\cos\phi)| \quad\text{..............(7).}$$

Now it is well known (see Heine, *Kugelfunctionen*, 2nd ed., p. 174) that if ϕ differs from 0 or π by a quantity not less than a fixed finite amount

$$P_n(\cos\phi) = \sqrt{\left(\frac{2}{n\pi\sin\phi}\right)} \sin\{(n+\tfrac{1}{2})\phi + \tfrac{1}{4}\pi\}$$

approximately when n is large. Hence

$$|P_n(\cos\phi)| < \frac{M}{\sqrt{n}},$$

where M is a fixed finite positive quantity. Thus

$$|R_n| < \frac{1}{\sqrt{n}} \frac{M}{b(1-b)} \frac{|X|^n}{(1-|X\cos\alpha|)^3},$$

and therefore approaches zero, when n increases, whenever $|X| \leq 1$.

6. It is interesting to note why the usual remainders fail with this series when $|X|=1$. Cauchy's remainder form would give

$$|R_n| = \left| \frac{X^n(1-\theta)^{n-1}}{(1-2\theta X\cos\alpha+\theta^2X^2)^{\frac{1}{2}(n+1)}}\, nP_n(\cos\phi) \right|$$

$$< \frac{|X|^n}{\{1-|X\cos\alpha|\}^2} \left(\frac{1-\theta}{1-\theta\,|X\cos\alpha|}\right)^{n-1} |nP_n(\cos\phi)|$$

$$< \frac{|X|^n}{\{1-|X\cos\alpha|\}^2} |nP_n(\cos\phi)|,$$

as before. But when $|X|=1$ this does not tend to zero when n increases, because $|nP_n(\cos\phi)|$ does not tend to zero.

Lagrange's remainder would give

$$|R_n| = \left| \frac{X^n}{(1-2\theta X\cos\alpha+\theta^2X^2)^{\frac{1}{2}(n+1)}}\, P_n(\cos\phi) \right|.$$

Now, if we put $X=1$ in this, we have the least value of $1-2\theta\cos\alpha+\theta^2$, given by $\theta=\cos\alpha$ or

$$|R_n| < \frac{1}{(\sin\alpha)^{n+1}} |P_n(\cos\phi)|,$$

and the right-hand side does not tend to zero as n increases.

It seems that the upper limit to the remainder, given by formula (4), combines to some extent the advantages of Cauchy's and Lagrange's forms, for, while giving $n!$ instead of $(n-1)!$ in the denominator, it nevertheless brings in a factor $(1-b\theta)^{n-2}$ which frequently enables one to make certain other factors occurring in the $f^n\{x+\theta(X-x)\}$ less than unity.

That the series for $(1-2x\cos\alpha+x^2)$ does represent the function when $|x|=1$ is of course well known, and is easily proved from Abel's theorem on the convergence of power series on their circle of convergence; but it seemed of some interest to deduce it directly from a remainder form of Taylor's theorem, especially as this form may be of value in other cases.

NOTES ON SOME POINTS IN THE INTEGRAL CALCULUS.

By *G. H. Hardy.*

XXXII.

On double series and double integrals.

1. It is easily proved that, if $f(x)$ is a function of x with a continuous derivative $f'(x)$, then

$$(1)\quad f(m)-\int_m^{m+1} f(x)\,dx=-\int_m^{m+1}(m+1-x)f'(x)\,dx,$$

$$(2)\quad \left|\sum_1^m f(m)-\int_1^{m+1} f(x)\,dx\right|\leq\int_1^{m+1}|f'(x)|\,dx.$$

The formulæ are capable of many interesting applications.*

In this note I propose to give the corresponding formulæ for double series and integrals, and to indicate a few simple applications of them.

2. Theorem 1. *If $f(x, y)$ has continuous derivatives* f_x, f_y, f_{xy}, then

$$f(m, n)-\int_m^{m+1}\int_n^{n+1} f(x, y)\,dx\,dy$$

$$=\int_m^{m+1}\int_n^{n+1}\left\{(m+1-x)(n+1-y)\frac{\partial^2 f}{\partial x\,\partial y}\right.$$

$$\left.-(m+1-x)\frac{\partial f}{\partial x}-(n+1-y)\frac{\partial f}{\partial y}\right\}dx\,dy.$$

As the proof of this is a matter of merely formal transformation by partial integration, I may leave it to the reader.

---

* See *Proc. Lond. Math. Soc.*, vol. ix., p. 126.

THEOREM 2. *Under similar conditions the absolute value of*

$$\sum_1^m \sum_1^n f(\mu, \nu) - \int_1^{m+1} \int_1^{n+1} f(x, y)\, dx\, dy$$

is not greater than

$$\int_1^{m+1} \int_1^{n+1} \left(\left|\frac{\partial f}{\partial x}\right| + \left|\frac{\partial f}{\partial y}\right| + \left|\frac{\partial^2 f}{\partial x\, \partial y}\right| \right) dx\, dy.$$

This follows at once from the fact that

$$0 \leqq m + 1 - x \leqq 1, \qquad 0 \leqq n + 1 - y \leqq 1$$

in the result of Theorem 1.

Applications.

3. (i) Let $\qquad f(x, y) = \dfrac{1}{(a + x\omega_1 + y\omega_2)^s}$.

where

$$R(a) > 0, \quad R(\omega_1) > 0, \quad R(\omega_2) > 0, \quad s \neq 1, \quad s \neq 2,$$

and $(a + x\omega_1 + y\omega_2)^{-s}$ has its principal value.* Then the conditions of the theorems are satisfied.

Let $\qquad m = p\lambda - 1, \quad n = q\lambda - 1,$

where p, q, and λ are positive integers. Then

$$\int_1^{p\lambda} \int_1^{q\lambda} \frac{dx\, dy}{(a + x\omega_1 + y\omega_2)^s} = \frac{1}{(1-s)(2-s)\,\omega_1\omega_2} \{(a + p\lambda\omega_1 + q\lambda\omega_2)^{2-s}$$

$$- (a + p\lambda\omega_1 + \omega_2)^{2-s} - (a + \omega_1 + q\lambda\omega_2)^{2-s} + (a + \omega_1 + \omega_2)^{2-s}\}.$$

If $R(s) > 2$, the series

$$\Sigma \frac{1}{(a + m\omega_1 + n\omega_2)^s}$$

is convergent.

---

* Cf. Barnes, "The theory of the double gamma function," *Phil. Trans. Roy. Soc.* (A), vol. cxcvi., pp. 314 *et seq.*

If $R(s) < 2$ and $\lambda \rightarrow \infty$,

$$\int_1^{p\lambda}\int_1^{q\lambda} \frac{dx\,dy}{(a + x\omega_1 + y\omega_2)^s}$$

$$\sim \frac{\lambda^{2-s}}{(1-s)(2-s)\,\omega_1\omega_2}\{(p\omega_1 + q\omega_2)^{2-s} - (p\omega_1)^{2-s} - (q\omega_2)^{2-s}\}.$$

Again $$\frac{\partial f}{\partial x} = -\frac{s\omega_1}{(a + x\omega_1 + y\omega_2)^{s+1}},$$

$$\left|\frac{\partial f}{\partial x}\right| < \frac{K}{(\alpha + x\rho_1 + y\rho_2)^{\sigma+1}},$$

where α, ρ_1, ρ_2, and σ are the real parts of a, ω_1, ω_2, and s; and it is easily verified that

$$\int_1^{p\lambda}\int_1^{q\lambda}\left|\frac{\partial f}{\partial x}\right| dx\,dy < K\lambda^{1-\sigma}.$$

Similarly $$\int_1^{p\lambda}\int_1^{q\lambda}\left|\frac{\partial f}{\partial y}\right| dx\,dy < K\lambda^{1-\sigma},$$

$$\int_1^{p\lambda}\int_1^{q\lambda}\left|\frac{\partial^2 f}{\partial x\,\partial y}\right| dx\,dy < K\lambda^{-\sigma}.$$

Hence, finally, we see that

$$\sum_1^{p\lambda}\sum_1^{q\lambda} \frac{1}{(a + m\omega_1 + n\omega_2)^s}$$

$$\sim \frac{\lambda^{2-s}}{(1-s)(2-s)\,\omega_1\omega_2}\{(p\omega_1 + q\omega_1)^{2-s} - (p\omega_1)^{2-s} - (q\omega_2)^{2-s}\}.*$$

4. (ii) Let $f(x, y) = \dfrac{1}{(ax^2 + 2hxy + by^2)^s}$,

where all the letters denote real numbers, and

$$a > 0, \quad ab - h^2 > 0, \quad s \leq 1.†$$

---

* For a complete asymptotic expansion see Barnes, *loc. cit.* The cases in which $s = 1$ or 2 require special treatment.

† If $s > 1$, we obtain a convergent series and integral.

Suppose first $s<1$; then*

$$\int_0^{p\lambda}\int_0^{q\lambda}\frac{dx\,dy}{(ax^2+2hxy+by^2)^s}$$

$$=\int_0^{\phi}\frac{d\theta}{(a\cos^2\theta+2h\cos\theta\sin\theta+b\sin^2\theta)^s}\int_0^{p\lambda\sec\theta}r^{1-2s}\,dr$$

$$+\int_{\phi}^{\frac{1}{2}\pi}\frac{d\theta}{(a\cos^2\theta+2h\cos\theta\sin\theta+b\sin^2\theta)^s}\int_0^{q\lambda\operatorname{cosec}\theta}r^{1-2s}\,dr,$$

where $\tan\phi=q/p$. Performing the integrations with respect to r, and putting $\tan\theta=t$ in the first integral and $\cot\theta=t$ in the second, we obtain

$$\frac{\lambda^{2-2s}}{2-2s}\left\{p^{2-2s}\int_0^{q/p}\frac{dt}{(a+2ht+bt^2)^s}+q^{2-2s}\int_0^{p/q}\frac{dt}{(at^2+2ht+b)^s}\right\};$$

and we see as in § 3 that this is an asymptotic formula for

$$\sum_1^{p\lambda}\sum_1^{q\lambda}\frac{1}{(am^2+2hmn+bn^2)^s}.$$

In particular

$$\sum_1^{p\lambda}\sum_1^{q\lambda}\frac{1}{(m^2+n^2)^s}\sim\frac{\lambda^{2-2s}}{2-2s}\left\{p^{2-2s}F\left(\frac{q}{p}\right)+q^{2-2s}F\left(\frac{p}{q}\right)\right\},$$

where
$$F(x)=\int_0^x\frac{dt}{(1+t^2)^s}.$$

When $s=1$, the argument requires a little modification of detail: we obtain

$$\sum_1^{p\lambda}\sum_1^{q\lambda}\frac{1}{am^2+2hmn+bn^2}\sim\log\lambda\int_0^{\frac{1}{2}\pi}\frac{d\theta}{a\cos^2\theta+2h\cos\theta\sin\theta+b\sin^2\theta}$$

$$=\frac{\log\lambda}{\sqrt{(ab-h^2)}}\arctan\frac{\sqrt{(ab-h^2)}}{h}.$$

* It is convenient to take zero instead of unity as the lower limit of our integrations; no difficulty is introduced by doing so when $s<1$.

5. (iii) Theorems 1 and 2 may also be applied to the determination of asymptotic formulæ which show how such series as

$$\Sigma\Sigma \frac{x^m y^n}{(a + m\omega_1 + n\omega_2)^s},$$

$$\Sigma\Sigma \frac{x^m y^n}{(am^2 + 2hmn + bm^2)^s}$$

behave as x and y tend to unity: the essence of the application lies in the establishment of asymptotic relations of the type

$$\Sigma\Sigma \frac{e^{-\alpha m - \beta n}}{(a + m\omega_1 + n\omega_2)^s} \sim \int_0^\infty \int_0^\infty \frac{e^{-\alpha x - \beta y}}{(a + x\omega_1 + y\omega_2)^s} dx\, dy,$$

$$\Sigma\Sigma \frac{e^{-\alpha m - \beta n}}{(am^2 + 2hmn + cn^2)^s} \sim \int_0^\infty \int_0^\infty \frac{e^{-\alpha x - \beta y}}{(ax^2 + 2hxy + by^2)^s} dx\, dy,$$

holding when $\alpha \to 0$, $\beta \to 0$. The analysis necessary is too detailed to be included here, my only object at present being to give a few simple examples of the use of the theorems. Among the results which I have found I may quote the following:

$$\Sigma\Sigma \frac{x^m y^n}{(a + m\omega_1 + n\omega_2)^s}$$

$$\sim \frac{\Gamma(1-s)}{\omega_1(1-y) - \omega_2(1-x)} \left\{ \left(\frac{\omega_1}{1-x}\right)^{1-s} - \left(\frac{\omega_2}{1-y}\right)^{1-s} \right\},$$

$$\Sigma\Sigma \frac{x^m y^n}{(am^2 + 2hmn + bn^2)^s} \sim \frac{K\Gamma(2-2s)}{\{(1-x)^2 + (1-y)^2\}^{1-s}},$$

where

$$K = \int_0^{\frac{1}{2}\pi} \frac{d\theta}{(a\cos^2\theta + 2h\cos\theta\sin\theta + b\sin^2\theta)^s \{\cos^2(\theta - \tau)\}^{1-s}},$$

$$\Sigma\Sigma \frac{x^m y^n}{m^2 + n^2} \sim \tfrac{1}{4}\pi \log\left\{\frac{1}{(1-x)^2 + (1-y)^2}\right\}.$$

Here a, ω_1, ω_2, s, h, b are subject to the same conditions as before, and x and y tend to unity in such a way that

$$\frac{1-y}{1-x} \to \tan\tau.$$

In this connection I may refer to a paper, "The singular points of functions of several variables," published in the *Proc. Lond. Math. Soc.*, vol. v., p. 342.

ON CYCLANT SUBSTITUTIONS.

By *Harold Hilton.*

§ 1. HERR O. TOEPLITZ suggests* two interesting types of homogeneous linear substitution, whose properties are briefly discussed in this paper.

The typical homogeneous linear substitution A of degree m is

$$x_i' = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{im}x_m \quad (i = 1, 2, \ldots, m).$$

If

$$a_{i1}X_1 + \ldots + a_{i\,i-1}X_{i-1} + (a_{ii} - \lambda')\,X_i + a_{i\,i+1}X_{i+1} + \ldots + a_{im}X_m = 0 \qquad (i = 1, 2, \ldots, m),$$

$(X_1, X_2, \ldots, X_m)$ is a *pole* of A corresponding to the root $\lambda = \lambda'$ of the *characteristic equation* of A

$$\begin{vmatrix} a_{11} - \lambda, & a_{12}, & \ldots, & a_{1m} \\ a_{21}, & a_{22} - \lambda, & \ldots, & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}, & a_{m2}, & \ldots, & a_{mm} - \lambda \end{vmatrix} = 0 \ldots\ldots \text{(i)}.$$

Let $(X_{1i}, X_{2i}, \ldots, X_{mi})$ be a pole corresponding to the root λ_i of equation (i), and suppose the determinant

$$\begin{vmatrix} X_{11}, & \ldots, & X_{1m} \\ \cdots & \cdots & \cdots \\ X_{m1}, & \ldots, & X_{mm} \end{vmatrix} \neq 0.$$

Then, if T^{-1} is the substitution

$$x_i' = X_{i1}x_1 + X_{i2}x_2 + \ldots + X_{im}x_m \quad (i = 1, 2, \ldots, m)$$

with this determinant, $T^{-1}AT = M$; where M is the multiplication

$$x_i' = \lambda_i x_i \quad (i = 1, 2, \ldots, m).$$

In fact, we readily verify that $T^{-1}A = MT^{-1}$.

Type I.

§ 2. In this type A is the substitution with matrix

$$\begin{vmatrix} \alpha_1, & \alpha_2, & \alpha_3, & \ldots, & \alpha_m \\ \alpha_m, & \alpha_1, & \alpha_2, & \ldots, & \alpha_{m-1} \\ \alpha_{m-1}, & \alpha_m, & \alpha_1, & \ldots, & \alpha_{m-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_2, & \alpha_3, & \alpha_4, & \ldots, & \alpha_1 \end{vmatrix},$$

* *Math. Annalen*, lxx. (1911), pp. 364–6.

so that $a_{ij} = \alpha_{j-i+1}$, if we suppose α_h and α_k identical when $h \equiv k \pmod m$.

We verify at once that, if ω is any m^{th} root of unity, $(\omega, \omega^2, \ldots, \omega^m)$ is a pole of A corresponding to the root $\alpha_1 + \alpha_2\omega + \alpha_3\omega^2 + \ldots + \alpha_m\omega^{m-1}$ of the equation (i).

Suppose ω is a *primitive* m^{th} root of unity (so that all the m^{th} roots are $\omega, \omega^2, \ldots, \omega^m$), and T^{-1} is the symmetric substitution of order 4* with matrix

$$\begin{vmatrix} \dfrac{\omega}{\sqrt{m}}, & \dfrac{\omega^2}{\sqrt{m}}, & \ldots, & \dfrac{\omega^m}{\sqrt{m}} \\ \dfrac{\omega^2}{\sqrt{m}}, & \dfrac{\omega^4}{\sqrt{m}}, & \ldots, & \dfrac{\omega^{2m}}{\sqrt{m}} \\ \cdots & \cdots & \cdots & \cdots \\ \dfrac{\omega^m}{\sqrt{m}}, & \dfrac{\omega^{2m}}{\sqrt{m}}, & \ldots, & \dfrac{\omega^{mm}}{\sqrt{m}} \end{vmatrix}.$$

Then $T^{-1}AT$ is a multiplication (§ 1).

We see then that every substitution of Type I. has the same poles and is transformable into a multiplication by the same symmetric substitution T of order 4.

§ 3. It follows that any two such substitutions A, B are permutable, as may be readily verified independently.

In fact, if $P = AB$,

$$p_{ij} = \Sigma\alpha_a\beta_b = \Sigma\beta_a\alpha_b.$$

the sum being taken for all values of a and b between 1 and m inclusive such that $a + b \equiv j - i + 2 \pmod m$.

It follows also from this that the product of two substitutions of Type I. is itself of Type I.

More generally, if $A, B, C, \ldots, K$ are r substitutions of Type I., and $ABC\ldots K = P$,

$$p_{ij} = \Sigma\alpha_a\beta_b\gamma_c\ldots\kappa_k$$

where $\qquad a + b + c + \ldots + k \equiv j - i + r \pmod m$;

i.e., p_{ij} is the coefficient of x^{j-i} in

$$(\alpha_1 + \alpha_2 x + \ldots + \alpha_m x^{m-1})(\beta_1 + \beta_2 x + \ldots + \beta_m x^{m-1})\ldots$$
$$\ldots(\kappa_1 + \kappa_2 x + \ldots + \kappa_m x^{m-1})\left(1 + \frac{1}{x^m} + \frac{1}{x^{2m}} + \ldots\right).$$

---

* T^2 is $(x_{m-1}, x_{m-2}, \ldots, x_2, x_1, x_m)$.

Type II.

§4. In this type A is the symmetric substitution with matrix

$$\begin{vmatrix} \alpha_1, & \alpha_2, & \alpha_3, & \ldots, & \alpha_m \\ \alpha_2, & \alpha_3, & \alpha_4, & \ldots, & \alpha_1 \\ \alpha_3, & \alpha_4, & \alpha_5, & \ldots, & \alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_m, & \alpha_1, & \alpha_2, & \ldots, & \alpha_{m-1} \end{vmatrix},$$

so that a_{ij} is α_{i+j-1}, if we suppose α_h and α_k identical when $h \equiv k \pmod m$.

A has a pole $(1, 1, 1, 1, \ldots, 1, 1)$ corresponding to the root $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \ldots + \alpha_{m-1} + \alpha_m$ of equation (i). If m is even, A has also a pole $(1, -1, 1, -1, \ldots, 1, -1)$ corresponding to the root $\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 + \ldots + \alpha_{m-1} - \alpha_m$ of equation (i).

Suppose ω is an m^{th} root of unity other than ± 1. Then we at once verify that A has a pole

$$(a + b,\ \omega^{-1}a + \omega b,\ \omega^{-2}a + \omega^2 b,\ \ldots,\ \omega^{-m+1}a + \omega^{m-1}b)$$

corresponding to the root ab of equation (i), and a pole

$$(a - b,\ \omega^{-1}a - \omega b,\ \omega^{-2}a - \omega^2 b,\ \ldots,\ \omega^{-m+1}a - \omega^{m-1}b)$$

corresponding to the root $-ab$ of equation (i), where a denotes

$$(\alpha_1 + \alpha_2\omega + \alpha_3\omega^2 + \ldots + \alpha_m\omega^{m-1})^{\frac{1}{2}}$$

and b denotes $\quad (\alpha_1 + \alpha_2\omega^{-1} + \alpha_3\omega^{-2} + \ldots + \alpha_m\omega^{-m+1})^{\frac{1}{2}}$.

The determinant formed (as in §1) by the m poles we have now obtained is readily seen to be different from zero. Hence A is transformable into a multiplication.

§5. If $P = AB$, where A and B are of Type II., we have

$$p_{ij} = \beta_i\alpha_j + \beta_{i+1}\alpha_{j+1} + \ldots + \beta_{i-1}\alpha_{j-1}.$$

Hence P is of Type I.*

Since A^2 is of Type I., A^2 is transformable into a multiplication by §2. Therefore so is A,† as proved in §4.

We may show similarly that the product of a substitution of Type I. and a substitution of Type II. is a substitution of Type II. Hence the product of r substitutions of Type II. is of Type I. or II. as r is even or odd. The inverse of a substitution of either type is a substitution of the same type.

* A and B are not permutable in general, as in the case of Type I.

† See *Mess. of Math.*, vol. xxxix. (1909), p. 26.

A TABLE OF COMPLEX PRIME FACTORS IN THE FIELD OF 8^{th} ROOTS OF UNITY.

By the late *C. E. Bickmore* and *O. Western*.
With an Introduction by *A. E. Western*.

1. Table I. below gives a complex prime factor

$$\pi = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$$

of every prime number p which is of the form $8m+1$, up to the limit of 25,000; ζ here is a primitive 8^{th} root of 1, so that

$$\zeta^4 = -1.$$

The conjugates of π are obtained from π by replacing ζ by the other primitive 8^{th} roots of 1, *i.e.* $\zeta^5 = -\zeta$, ζ^3, and $\zeta^7 = -\zeta^3$.

They are
$$\pi_1 = a_0 - a_1\zeta + a_2\zeta^2 - a_3\zeta^3,$$
$$\pi_1{}^{\dagger} = a_0 + a_3\zeta - a_2\zeta^2 + a_1\zeta^3,$$
$$\pi^{\dagger} = a_0 - a_3\zeta - a_2\zeta^2 - a_1\zeta^3.$$

Then
$$p = \pi\pi_1\pi^{\dagger}\pi^{\dagger}{}_1.$$

It is easily seen that a_0 may be taken to be positive, and that one of the four conjugate factors may be chosen so that the coefficients of ζ and ζ^3 are also positive; then the coefficient of ζ^3 may be either positive or negative; this is the factor given in the Table.

2. The number
$$\epsilon = 1 + \zeta + \zeta^{-1}$$
is a unit, *i.e.* a divisor of 1, for

$$\epsilon\epsilon_1 = 1 - (\zeta - \zeta^3)^2 = -1.$$

It is in fact the fundamental unit in this field; that is, every unit is given by $\zeta^x\epsilon^y$, where y is any integer positive or negative. Since p is odd, either one or three of the coefficients of π must be odd; if one only is odd, by multiplying π by a suitable power of ζ, we can make a_0 the odd coefficient. And if one coefficient only is even, we can similarly make a_2 the even coefficient. In the latter case, we have

$$\pi \equiv 1 + \zeta + \zeta^3 \equiv \epsilon \pmod 2,$$

And then
$$\epsilon\pi \equiv \epsilon^2 \equiv 1 \pmod 2.$$

Therefore by multiplying π by the unit ϵ this case is reduced to the former case. When $\pi \equiv 1 \pmod 2$, so that

$$a_0 \equiv 1,\ a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod 2,$$

I have called this the *canonical* form of π*. The factors given in Table I. are in the canonical form.

3. Writing

$$\iota=\zeta^2=\sqrt{(-1)},\ \omega=\zeta+\zeta^3=\sqrt{(-2)},\ \varpi=\zeta-\zeta^3=\sqrt{2},$$

we obtain by multiplying π by each of its conjugates the following factors of p;

$$\pi\pi_1=a+b\iota,$$

where
$$\left.\begin{aligned} a&=\ \ a_0^2-a_2^2+2a_1a_3 \\ b&=-a_1^2+a_3^2+2a_0a_2 \end{aligned}\right\}\ldots\ldots\ldots\ldots\ldots\ldots(1),$$

$$\pi\pi_1{}^\dagger=c+d\omega,$$

where
$$\left.\begin{aligned} c&=a_0^2-a_1^2+a_2^2-a_3^2 \\ d&=a_1(a_0-a_2)+a_3(a_0+a_2) \end{aligned}\right\}\ldots\ldots\ldots\ldots(2),$$

and
$$\pi\pi^\dagger=e+f\varpi$$

where
$$\left.\begin{aligned} e&=a_0^2+a_1^2+a_2^2+a_3^2 \\ f&=a_1(a_0+a_2)-a_3(a_0-a_2) \end{aligned}\right\}\ldots\ldots\ldots\ldots(3).$$

These three formulæ give the following quadratic representations of p:

$$p=a^2+b^2=c^2+2d^2=e^2-2f^2.\dagger$$

In Lt.-Col. A. Cunningham's "Quadratic Partitions"‡ there are given for all values of p, not exceeding 25,000, the corresponding values of a, b, and c, d, (all which are unique except as to signs), and the least values of e, f.

4. With the definitions given above, we find, for a canonical π, that

$$a\equiv1,\ c\equiv1,\ e\equiv1,\ d\equiv f\pmod 4.$$

We therefore take a and c from Cunningham's tables with such sign as to satisfy these congruences. As regards e, the tabulated value may be $\equiv -1 \pmod 4$, which corresponds to a non-canonical form of π; to obtain the least values of e, f, corresponding to a canonical π, we take

$$e+f\varpi=\epsilon^{-2}(e'+f'\varpi),$$

where e', f' have the tabulated values in Cunningham's tables, and
$$\epsilon^{-2}=(1-\varpi)^2=3-2\varpi.$$

* "An Extension of Eisenstein's Law of Reciprocity," *Proc. London Math. Society*, series 2, vol. vi., p. 265; see as to the field of 8th roots of 1, §§ 29, 30

† See Bickmore, "On the Numerical Factors of a^n-1," *Messenger of Maths*, vol. xxvi., p. 13.

‡ *London*, 1904.

Then
$$\left.\begin{aligned} e &= 3e' - 4f' \\ f &= 2e' - 3f' \end{aligned}\right\} \quad \text{(4)}.$$

Table I. gives besides π the corresponding values of e, f.

5. With these data the calculation of π becomes a simple matter. From (2) and (3) we obtain

$$a_0^2 + a_2^2 = \tfrac{1}{2}(e + c) \quad \text{(5)},$$
$$a_1^2 + a_3^2 = \tfrac{1}{2}(e - c) \quad \text{(6)}.$$

Table III. below gives all integral solutions of

$$x^2 + y^2 = n,$$

for all values of n, for which any solution exists, not exceeding 1000. From this table the solutions of (5) and (6) are at once found; and, since a_0 is odd and a_2 is even, these are distinguishable; all that remains is to find which of the possible values of a_0, a_1, a_2, and $\pm a_3$ thus obtained satisfy

$$(a_0 + a_2)\, a_1 - (a_0 - a_2)\, a_3 = \pm f.$$

For instance, $p = 24{,}841$. Here $c = -127$, $e' = 179$, $f' = 60$, and so $e = 297$, $f = 178$. Then

$$a_0^2 + a_2^2 = 85 = 9^2 + 2^2 = 7^2 + 6^2$$

and
$$a_1^2 + a_3^2 = 212 = 14^2 + 4^2.$$

We try first $a_0 = 9$, $a_2 = 2$, which gives

$$11a_1 - 7a_3 = \pm 178;$$

this is not satisfied by $a_1 = 14$, $a_3 = \pm 4$, nor by $a_1 = 4$, $a_3 = \pm 14$. So $a_0 = 7$, $a_2 = 6$, which gives

$$13a_1 - a_3 = 178,$$

which is satisfied by $a_1 = 14$, $a_3 = 4$, and so

$$\pi = 7 + 14\zeta + 6\zeta^2 + 4\zeta^3.$$

6. As mentioned above, a canonical π may correspond to a value of e which is not the least value. Whenever this is the case, a complex prime factor of p, say π', exists corresponding to the least value of e, and from (3) we see that the sum of the squares of the coefficients of π' is equal to this least value of e. I therefore call π' a *simplest* prime factor of p. For some purposes, a prime factor of p may be needed in its canonical form; but for other purposes it is more convenient to use the simplest form, as the numbers involved are smaller. It will be seen from (4) that if π'

is the same factor of p as π, but differs by a unit, then the connection between π' and π is $\pi' = \epsilon^{\pm 1}\pi$.

Table II. contains a simplest factor of p for all values of p of the form $16m+1$ up to 10,000, but omitting those values of p for which the simplest factor of p is already given in Table I. The simplest factors have been calculated directly, by the same process as that described above, but using the least values of e, f, as given in Cunningham's "Quadratic Partitions."

7. Tables I. and II. may be used in connection with the evaluation of

$$q^{\frac{1}{8}(p-1)} \quad (\mathrm{mod}\, p),$$

a problem which depends upon the Law of Reciprocity

$$\{q/\pi\}_8 = \{\pi/q\}_8.*$$

I have also found these tables useful in the calculation of a similar table of prime factors of p in the field of 16^{th} roots of 1.

8. Table I. was calculated by the late Mr. C. E. Bickmore up to $p = 20{,}353$; after his death his manuscript was acquired from his widow by Lt.-Col. A. Cunningham, who partially checked it; Mr. O. Western has also checked it and corrected errors and omissions, and has calculated the factors of the remaining primes up to 25,000.

Table II. was calculated by the writer. The prime factor given in this table for a given prime p will generally not be the same prime factor as that given in Table I., but one of its conjugates multiplied by ϵ or ϵ^{-1}.

9. The only previously existing table of prime factors in the field of 8^{th} roots of 1 is included in C. G. Reuschle's *Tafeln Complexer Primzahlen* (Berlin, 1875), at p. 443. This only contains primes under 1000. Reuschle has given no details of his method of calculation, but a comparison between his table and the present tables suggests that his method was: (i) whenever possible, to calculate a factor π of the form $a_0 + a_1\zeta + a_3\zeta^3$: that is, with the coefficient $a_2 = 0$; (ii) in the remaining cases, to calculate the simplest factor. As Reuschle remarks in a footnote, the expression of π in a three-termed form often involves large values of the coefficients.

* See "Some Criteria for the Residues of Eighth and other Powers," *Proc. London Math. Society*, series 2, vol. ix., p. 244.

Canonical prime factors. TABLE I.

p	a_0 a_1 a_2 a_3	e f	p	a_0 a_1 a_2 a_3	e f
17	1, 2, 0, 0	5, 2	1433	5, 4, 2, 2	49, 22
41	1, 2, 2, 2	13, 8	1481	1, 0, 6, 2	41, 10
73	1, 0, 2, 2	9, 2	1489	7, 6, 4, 0	101, 66
89	3, 2, 2, 0	17, 10	1553	1, 6, 0, −2	41, 8
97	3, 2, 0, 0	13, 6	1601	5, 2, 4, −2	49, 20
113	1, 2, 4, 2	25, 16	1609	1, 0, 2, 6	41, 6
137	1, 2, 2, −2	13, 4	1657	3, 2, 6, 2	53, 24
193	3, 4, 0, −2	29, 18	1697	3, 6, 4, 4	77, 46
233	1, 4, 2, 2	25, 14	1721	5, 8, 2, −2	97, 62
241	1, 2, 4, 0	21, 10	1753	3, 2, 6, 0	49, 18
257	1, 4, 0, 0	17, 4	1777	1, 6, 8, 2	105, 68
281	3, 0, 2, 2	17, 2	1801	1, 6, 6, 0	73, 42
313	3, 2, 2, 2	21, 8	1873	1, 4, 4, 6	69, 38
337	3, 4, 0, 0	25, 12	1889	5, 2, 4, 2	49, 16
353	1, 4, 4, 4	49, 32	1913	3, 6, 2, −4	65, 34
401	1, 2, 4, 4	37, 22	1993	1, 2, 6, −2	45, 4
409	1, 0, 2, 4	21, 4	2017	5, 0, 4, 2	45, 2
433	1, 4, 0, 2	21, 2	2081	5, 8, 4, 2	109, 70
449	3, 2, 4, 0	29, 14	2089	7, 6, 2, 0	89, 54
457	5, 4, 2, 0	45, 28	2113	3, 6, 0, 2	49, 12
521	5, 4, 2, −4	61, 40	2129	5, 4, 4, −4	73, 40
569	5, 2, 2, −2	37, 20	2137	1, 8, 6, 4	117, 76
577	3, 2, 4, 2	33, 16	2153	7, 2, 2, −2	61, 28
593	1, 2, 4, −2	25, 4	2161	1, 0, 4, 6	53, 18
601	3, 6, 2, 0	49, 30	2273	1, 4, 4, −4	49, 8
617	1, 2, 2, −4	25, 2	2281	1, 6, 2, 4	57, 22
641	5, 2, 0, 0	29, 10	2297	3, 2, 2, −6	53, 16
673	3, 4, 4, −2	45, 26	2377	5, 8, 2, 0	93, 56
761	3, 6, 2, −2	53, 32	2393	5, 2, 2, 4	49, 2
769	3, 4, 0, 2	29, 6	2417	7, 2, 0, 0	53, 14
809	3, 0, 2, 4	29, 4	2441	7, 2, 2, −4	73, 38
857	1, 4, 2, 4	37, 16	2473	7, 6, 6, 0	121, 78
881	5, 4, 0, 0	41, 20	2521	3, 2, 6, −2	53, 12
929	5, 6, 0, −4	77, 50	2593	3, 6, 8, 6	145, 96
937	1, 2, 6, 4	57, 34	2609	1, 6, 0, −4	53, 10
953	7, 4, 2, −4	85, 56	2617	3, 6, 6, −2	85, 48
977	1, 4, 4, −2	37, 14	2633	5, 8, 2, −4	109, 68
1009	1, 6, 4, 0	53, 30	2657	7, 4, 0, 0	65, 28
1033	1, 6, 2, 0	41, 18	2689	7, 4, 4, 0	81, 44
1049	5, 2, 2, −4	49, 26	2713	5, 2, 2, −6	69, 32
1097	7, 4, 2, −2	73, 46	2729	3, 8, 2, 0	77, 40
1129	3, 4, 6, 0	61, 36	2753	5, 2, 4, −4	61, 22
1153	5, 6, 4, 2	81, 52	2777	3, 2, 2, 6	53, 4
1193	1, 4, 6, 6	89, 58	2801	1, 6, 0, 4	53, 2
1201	3, 4, 4, 4	57, 32	2833	3, 4, 8, 4	105, 64
1217	1, 4, 8, 4	97, 64	2857	1, 6, 2, −4	57, 14
1249	3, 6, 0, −2	49, 24	2897	1, 8, 8, 2	133, 86
1289	1, 2, 6, 0	41, 14	2953	5, 8, 6, 4	141, 92
1297	1, 6, 0, 0	37, 6	2969	5, 6, 6, 4	113, 70
1321	3, 4, 6, 4	77, 48	3001	5, 6, 2, −6	101, 60
1361	1, 2, 4, −4	37, 2	3041	3, 6, 4, −4	77, 38
1409	5, 4, 4, 2	61, 34	3049	7, 0, 2, 2	57, 10

Canonical prime factors. TAB. I. (*cont.*)

p	$a_0\ a_1\ a_2\ a_3$	$e\ f$	p	$a_0\ a_1\ a_2\ a_3$	$e\ f$
3089	5, 8, 4, −4	121, 76	4817	7, 2, 4, 2	73, 16
3121	1, 2, 4, −6	57, 8	4889	1, 4, 10, 4	133, 80
3137	7, 4, 4, −4	97, 56	4937	1, 2, 2, 8	73, 14
3169	3, 6, 8, 0	109, 66	4969	9, 10, 2, −2	189, 124
3209	5, 4, 2, 4	61, 16	4993	1, 0, 8, 4	81, 28
3217	5, 0, 4, 4	57, 4	5009	9, 10, 4, 0	197, 130
3257	5, 2, 6, 0	65, 22	5081	5, 6, 6, −4	113, 62
3313	1, 6, 4, 6	89, 48	5113	3, 10, 6, 4	161, 102
3329	5, 2, 4, 4	61, 14	5153	5, 4, 8, 2	109, 58
3361	1, 8, 4, 0	81, 40	5209	5, 2, 6, 4	81, 26
3433	3, 0, 6, 4	61, 12	5233	9, 6, 4, −6	169, 108
3449	3, 6, 10, 4	161, 106	5273	3, 6, 10, 2	149, 92
3457	5, 6, 8, 0	125, 78	5281	3, 8, 0, 2	77, 18
3529	1, 0, 6, 6	73, 30	5297	1, 2, 8, −2	73, 4
3593	7, 2, 2, 2	61, 8	5393	5, 8, 4, 4	121, 68
3617	3, 4, 4, 6	77, 34	5417	1, 2, 6, −6	77, 16
3673	3, 8, 2, 2	81, 38	5441	5, 8, 8, −2	157, 98
3697	7, 6, 0, 0	85, 42	5449	5, 4, 6, −4	93, 40
3761	7, 2, 4, −2	73, 28	5521	9, 6, 4, 0	133, 78
3769	3, 10, 6, 2	149, 96	5569	5, 6, 4, −6	113, 60
3793	7, 2, 4, 0	69, 22	5641	1, 6, 2, −6	77, 12
3833	3, 4, 2, 6	65, 14	5657	1, 8, 2, 4	85, 28
3881	1, 6, 6, −2	77, 32	5689	5, 8, 2, −6	129, 74
3889	7, 8, 0, −2	117, 70	5737	7, 6, 2, −8	153, 94
3929	1, 8, 6, 0	101, 56	5801	3, 0, 2, 8	77, 8
4001	1, 8, 4, 4	97, 52	5849	1, 4, 10, 8	181, 116
4049	3, 4, 8, 0	89, 44	5857	5, 0, 4, 6	77, 6
4057	3, 8, 6, −2	113, 66	5881	3, 6, 6, −4	97, 42
4073	7, 6, 6, 2	125, 76	5897	5, 0, 6, 4	77, 4
4129	3, 8, 0, −2	77, 30	5953	5, 8, 8, 6	189, 122
4153	3, 2, 6, −4	65, 6	6073	3, 6, 2, 6	85, 24
4177	3, 8, 0, 0	73, 24	6089	1, 8, 10, 2	169, 106
4201	1, 4, 10, 6	153, 98	6113	11, 8, 4, −2	205, 134
4217	5, 0, 6, 2	65, 2	6121	7, 0, 2, 6	89, 30
4241	7, 8, 4, 2	133, 82	6217	9, 6, 6, −2	157, 96
4273	9, 6, 0, −2	121, 72	6257	1, 4, 8, −2	85, 22
4289	9, 8, 4, 0	161, 104	6329	9, 4, 2, 0	101, 44
4297	9, 4, 2, −2	105, 58	6337	3, 4, 8, −2	93, 34
4337	7, 4, 4, 2	85, 38	6353	7, 6, 0, 2	89, 28
4409	5, 8, 2, 2	97, 50	6361	5, 4, 2, 6	81, 10
4441	1, 4, 6, 8	117, 68	6449	5, 4, 8, 4	121, 64
4457	9, 6, 2, −8	185, 122	6473	5, 4, 2, −8	109, 52
4481	1, 8, 8, 8	193, 128	6481	7, 6, 8, 2	153, 92
4513	3, 2, 8, 2	81, 32	6521	5, 2, 2, −8	97, 38
4561	1, 8, 0, −2	69, 10	6529	1, 8, 0, 4	81, 4
4649	7, 10, 2, −2	157, 100	6553	3, 2, 2, 8	81, 2
4657	7, 6, 4, −6	137, 84	6569	7, 2, 6, 0	89, 26
4673	3, 4, 8, 6	125, 74	6577	9, 2, 0, 0	85, 18
4721	5, 8, 0, 0	89, 40	6673	1, 0, 8, 6	101, 42
4729	5, 2, 2, 6	69, 4	6689	9, 8, 8, 0	209, 136
4793	7, 4, 6, 0	101, 52	6737	1, 2, 8, 8	133, 74
4801	3, 6, 4, 6	97, 48	6761	7, 8, 10, 2	217, 142

Canonical prime factors. TAB. I. (*cont.*)

p	a_0 a_1 a_2 a_3	e f
6793	1, 8, 6, −2	105, 46
6833	1, 2, 4, −8	85, 14
6841	5, 10, 2, 0	129, 70
6857	7, 12, 6, 2	233, 154
6961	1, 8, 4, 6	117, 58
6977	5, 10, 4, −4	157, 94
7001	1, 0, 6, 8	101, 40
7057	9, 10, 0, −4	197, 126
7121	3, 0, 8, 4	89, 20
7129	5, 6, 10, 4	177, 110
7177	5, 12, 6, 0	205, 132
7193	1, 4, 2, −8	85, 4
7297	5, 2, 8, 0	93, 26
7321	5, 6, 6, 6	133, 72
7369	9, 10, 6, 2	221, 144
7393	3, 10, 4, −2	129, 68
7417	7, 4, 6, −4	117, 56
7433	9, 2, 2, −6	125, 64
7457	3, 6, 8, 8	173, 106
7481	11, 8, 2, −2	193, 122
7489	5, 6, 8, 6	161, 96
7529	9, 0, 2, 2	89, 14
7537	9, 10, 0, −8	245, 162
7561	9, 10, 6, −6	253, 168
7577	5, 10, 2, −4	145, 82
7649	5, 4, 8, −2	109, 46
7673	7, 8, 2, −8	181, 112
7681	3, 2, 4, 8	93, 22
7753	9, 6, 6, −4	169, 102
7793	3, 0, 4, 8	89, 8
7817	7, 6, 6, 4	137, 74
7841	1, 8, 4, −4	97, 28
7873	11, 6, 4, −4	189, 118
7937	3, 8, 4, 6	125, 62
7993	11, 8, 6, −2	225, 146
8009	5, 8, 2, 4	109, 44
8017	7, 10, 0, −4	165, 98
8081	3, 12, 8, 4	233, 152
8089	3, 10, 6, −2	149, 84
8161	5, 6, 4, 6	113, 48
8209	5, 8, 12, 4	249, 164
8233	9, 8, 6, 2	185, 114
8273	11, 8, 4, −8	265, 176
8297	3, 8, 10, 0	173, 104
8329	1, 2, 10, 6	141, 76
8353	3, 8, 0, −6	109, 42
8369	1, 10, 4, 2	121, 56
8377	7, 8, 10, 0	213, 136
8513	3, 12, 8, 2	221, 142
8521	9, 2, 2, 2	93, 8
8537	3, 8, 2, −6	113, 46
8609	5, 2, 8, −2	97, 20
8641	3, 2, 8, −4	93, 2
8681	1, 2, 10, 2	109, 40
8689	1, 10, 4, 0	117, 50
8713	7, 6, 2, 4	105, 34
8737	11, 10, 0, −4	237, 154
8753	9, 4, 4, −6	149, 82
8761	3, 4, 6, −6	97, 18
8849	9, 2, 4, 0	101, 26
8929	3, 10, 4, 4	141, 74
8969	1, 10, 6, 0	137, 70
9001	9, 8, 6, −6	217, 138
9041	1, 6, 12, 4	197, 122
9049	5, 6, 2, 6	101, 24
9137	7, 10, 0, −6	185, 112
9161	11, 4, 2, −4	157, 88
9209	5, 2, 2, 8	97, 10
9241	3, 2, 6, 8	113, 42
9257	1, 10, 10, 2	205, 128
9281	1, 4, 8, −4	97, 8
9337	5, 0, 6, 6	97, 6
9377	1, 4, 4, −8	97, 4
9433	3, 10, 6, 6	181, 108
9473	7, 8, 4, 4	145, 76
9497	5, 10, 2, 2	133, 64
9521	9, 6, 4, 2	137, 68
9601	3, 10, 12, 2	257, 168
9649	1, 6, 8, 10	201, 124
9689	5, 2, 6, −6	101, 16
9697	11, 6, 4, −2	177, 104
9721	5, 6, 10, 0	161, 90
9769	1, 12, 10, 6	281, 186
9817	1, 4, 10, 0	117, 44
9833	1, 10, 2, 2	109, 32
9857	5, 10, 4, 4	157, 86
9929	1, 10, 6, 6	173, 100
10009	5, 6, 10, 6	197, 120
10169	7, 0, 6, 4	101, 4
10177	3, 10, 0, −2	113, 36
10193	1, 8, 0, 6	101, 2
10273	3, 6, 12, 4	205, 126
10289	1, 4, 8, 10	181, 106
10313	1, 10, 2, −2	109, 28
10321	9, 10, 4, −8	261, 170
10337	7, 8, 8, −4	193, 116
10369	1, 0, 8, 8	129, 56
10433	11, 6, 0, −2	161, 88
10457	3, 8, 2, 6	113, 34
10513	9, 2, 4, 2	105, 16
10529	5, 2, 4, −8	109, 26
10601	1, 10, 10, 10	301, 200
10657	9, 8, 0, 0	145, 72
10729	3, 0, 6, 8	109, 24

Canonical prime factors. TAB. I. (*cont.*)

p	a_0 a_1 a_2 a_3	e f
10753	3, 8, 12, 2	221, 138
10889	1, 2, 10, 8	169, 94
10937	11, 8, 6, −6	257, 166
10993	7, 2, 4, 6	105, 4
11057	13, 8, 4, −4	265, 172
11113	9, 0, 2, 6	121, 42
11161	13, 6, 2, −8	273, 178
11177	1, 4, 10, 10	217, 134
11257	3, 12, 6, 2	193, 114
11273	11, 4, 2, −8	205, 124
11321	5, 10, 10, 8	289, 190
11329	3, 10, 8, −2	177, 100
11353	13, 6, 2, −6	245, 156
11369	1, 2, 2, 10	109, 16
11393	3, 6, 8, −4	125, 46
11489	5, 2, 8, −4	109, 14
11497	3, 8, 6, 8	173, 96
11593	1, 6, 6, −6	109, 12
11617	3, 10, 0, 2	113, 24
11633	5, 8, 8, −4	169, 92
11657	9, 12, 2, −2	233, 146
11681	5, 2, 4, 8	109, 10
11689	1, 2, 6, 10	141, 64
11777	7, 4, 4, −8	145, 68
11801	3, 6, 2, 8	113, 22
11833	9, 4, 6, −4	149, 72
11897	5, 10, 6, 6	197, 116
11953	9, 6, 8, 0	181, 102
11969	9, 0, 4, 4	113, 20
12041	7, 4, 6, −6	137, 58
12049	9, 6, 0, 2	121, 36
12073	9, 8, 2, −10	249, 158
12097	3, 10, 0, −4	125, 42
12113	1, 8, 8, 10	229, 142
12161	7, 8, 4, −8	193, 112
12241	3, 12, 8, 0	217, 132
12281	7, 8, 2, 4	133, 52
12289	3, 8, 12, 10	317, 210
12329	1, 10, 2, 4	121, 34
12377	3, 0, 10, 2	113, 14
12401	7, 10, 0, 0	149, 70
12409	3, 10, 2, 4	129, 46
12433	7, 6, 8, −4	165, 86
12457	9, 8, 2, 2	153, 74
12473	5, 8, 6, −6	161, 82
12497	9, 2, 4, −6	137, 56
12553	7, 12, 2, −2	201, 118
12569	3, 0, 2, 10	113, 10
12577	7, 12, 8, −4	273, 176
12601	7, 12, 2, −4	213, 128
12641	3, 2, 8, −6	113, 8
12689	1, 4, 4, 10	133, 50
12697	3, 2, 6, −8	113, 6
12713	7, 14, 6, 0	281, 182
12721	1, 8, 4, −6	117, 22
12809	5, 8, 10, 8	253, 160
12841	9, 2, 6, 0	121, 30
12889	3, 2, 2, −10	117, 20
12953	3, 2, 10, 6	149, 68
13001	1, 6, 6, 10	173, 92
13009	9, 10, 8, 4	261, 166
13033	9, 2, 6, −2	125, 36
13049	5, 8, 10, −2	193, 110
13121	5, 10, 0, −6	161, 80
13177	9, 4, 2, 4	117, 16
13217	11, 14, 4, −2	337, 224
13241	5, 10, 10, −2	229, 140
13249	5, 12, 4, 2	189, 106
13297	1, 10, 0, −4	117, 14
13313	3, 6, 4, −8	125, 34
13337	11, 2, 2, −4	145, 62
13417	7, 6, 10, 0	185, 102
13441	5, 10, 0, 2	129, 40
13457	7, 2, 4, −8	133, 46
13513	7, 14, 6, −2	285, 184
13537	11, 6, 4, −8	237, 146
13553	7, 10, 4, 4	181, 98
13577	7, 2, 6, −6	125, 32
13633	1, 12, 8, 4	225, 136
13649	7, 10, 12, 0	293, 190
13681	7, 0, 8, 2	117, 2
13697	11, 4, 4, −2	157, 74
13721	11, 6, 6, −2	197, 112
13729	11, 6, 4, 0	173, 90
13841	1, 2, 4, −10	121, 20
13873	9, 14, 4, −4	309, 202
13913	11, 6, 6, −4	209, 122
13921	3, 6, 12, 2	193, 108
14009	3, 6, 10, −2	149, 64
14033	7, 14, 8, 4	325, 214
14057	3, 0, 10, 4	125, 28
14081	11, 8, 8, −2	253, 158
14153	7, 14, 10, −2	349, 232
14177	5, 10, 8, −4	205, 118
14249	1, 2, 10, −4	121, 14
14281	7, 6, 6, 6	157, 72
14321	5, 8, 8, 8	217, 128
14369	3, 10, 4, 6	161, 76
14401	9, 4, 4, −8	177, 92
14419	3, 12, 4, 0	169, 84
14489	5, 2, 10, 2	133, 40
14537	7, 4, 6, 6	137, 46
14561	5, 10, 12, 0	269, 170
14593	9, 4, 4, 4	129, 32

Canonical prime factors. TAB. I. (*cont.*)

p	a_0 a_1 a_2 a_3	e f	p	a_0 a_1 a_2 a_3	e f
14633	1, 4, 2, −10	121, 2	16553	1, 12, 6, 2	185, 94
14657	11, 2, 0, 0	125, 22	16561	9, 10, 0, 0	181, 90
14713	13, 6, 2, −4	225, 134	16633	3, 2, 10, −4	129, 2
14737	5, 12, 12, 0	313, 204	16649	15, 8, 2, −6	329, 214
14753	7, 4, 8, −4	145, 56	16657	7, 12, 8, 6	293, 186
14897	11, 4, 0, 0	137, 44	16673	9, 4, 8, 0	161, 68
14929	9, 10, 12, 2	329, 216	16729	5, 12, 10, −2	273, 170
14969	5, 6, 6, 8	161, 74	16889	5, 2, 10, −2	133, 20
15017	7, 8, 6, 6	185, 98	16921	11, 10, 6, 2	261, 160
15073	7, 8, 0, 4	129, 28	16937	1, 2, 10, 10	205, 112
15121	15, 10, 0, −6	361, 240	16993	3, 4, 4, 10	141, 38
15137	3, 12, 4, 2	173, 86	17033	7, 10, 14, 4	361, 238
15161	9, 12, 2, −8	293, 188	17041	9, 6, 0, 4	133, 18
15193	3, 8, 6, −6	145, 54	17137	7, 10, 0, 2	153, 56
15217	3, 8, 4, 8	153, 64	17209	3, 4, 6, 10	161, 66
15233	3, 4, 8, −6	125, 14	17257	9, 14, 6, 2	317, 204
15241	9, 2, 6, −4	137, 42	17321	7, 8, 2, −10	217, 122
15289	11, 2, 2, 0	129, 26	17377	13, 6, 4, −6	257, 156
15313	5, 12, 4, −4	201, 112	17393	9, 12, 4, 2	245, 146
15329	5, 14, 8, 4	301, 194	17401	9, 0, 6, 4	133, 12
15361	7, 8, 12, 4	273, 172	17417	1, 8, 6, −6	137, 26
15377	7, 2, 8, 4	133, 34	17449	3, 12, 2, 0	157, 60
15401	7, 2, 2, −10	157, 68	17489	1, 4, 4, −10	133, 10
15473	9, 6, 4, 4	149, 58	17497	3, 0, 10, 6	145, 42
15497	5, 0, 6, 8	125, 8	17569	5, 4, 8, −6	141, 34
15569	3, 0, 8, 8	137, 40	17609	7, 4, 10, 2	169, 74
15601	1, 12, 8, 2	213, 122	17657	7, 4, 2, 8	133, 4
15641	1, 8, 2, 8	133, 32	17681	7, 2, 4, 8	133, 2
15649	5, 6, 4, 8	141, 46	17713	9, 10, 12, 4	341, 222
15737	11, 10, 10, −2	325, 212	17729	3, 10, 4, −6	161, 64
15761	5, 8, 4, −8	169, 80	17737	7, 12, 6, −6	265, 162
15809	11, 10, 8, 2	289, 184	17761	3, 4, 12, 2	173, 78
15817	5, 12, 2, 0	173, 84	17881	3, 2, 10, 8	177, 82
15881	9, 6, 2, 4	137, 38	17921	11, 2, 4, −4	157, 58
15889	9, 0, 4, 6	133, 30	17929	1, 8, 6, 10	201, 106
15913	1, 6, 14, 6	269, 168	17977	7, 4, 10, 0	165, 68
15937	11, 6, 0, 0	157, 66	18041	11, 2, 2, −8	193, 98
16001	13, 10, 8, −4	349, 230	18049	3, 4, 8, 10	189, 94
16033	3, 4, 12, 6	205, 114	18089	7, 10, 6, 6	221, 124
16057	11, 14, 2, −6	357, 236	18097	9, 12, 12, −2	373, 246
16073	5, 12, 6, −4	221, 128	18121	9, 2, 6, 4	137, 18
16097	11, 12, 0, −10	365, 242	18169	5, 8, 14, 6	321, 206
16193	9, 12, 4, −8	305, 196	18217	15, 10, 6, −6	397, 264
16217	3, 6, 10, 10	245, 148	18233	3, 12, 2, −2	161, 62
16249	5, 2, 6, −8	129, 14	18257	1, 10, 0, −6	137, 16
16273	1, 4, 12, 2	165, 74	18289	3, 8, 12, 0	217, 120
16361	1, 10, 14, 4	313, 202	18313	1, 6, 2, 10	141, 28
16369	9, 8, 0, 2	149, 54	18329	3, 10, 2, 6	149, 44
16417	3, 10, 0, −6	145, 48	18353	9, 14, 4, −6	329, 212
16433	11, 8, 8, −4	265, 164	18401	11, 8, 4, −10	301, 190
16481	3, 12, 4, −2	173, 82	18433	3, 6, 8, −6	145, 36
16529	7, 10, 4, −8	229, 134	18457	3, 10, 10, −2	213, 116

Canonical prime factors. TAB. I. (cont.)

p	a_0 a_1 a_2 a_3	e f	p	a_0 a_1 a_2 a_3	e f
18481	1, 6, 8, −6	137, 12	20681	11, 4, 6, 0	173, 68
18521	11, 14, 2, −4	337, 218	20753	7, 14, 8, −4	325, 206
18553	9, 8, 6, −8	245, 144	20809	9, 12, 10, 6	361, 234
18593	7, 12, 0, −4	209, 112	20849	1, 2, 12, 0	149, 26
18617	5, 14, 6, 0	257, 154	20857	3, 4, 10, 10	225, 122
18713	11, 4, 2, 2	145, 34	20873	7, 4, 10, −2	169, 62
18793	9, 2, 2, −10	189, 92	20897	5, 2, 4, 10	145, 8
18913	11, 4, 0, 2	141, 22	20921	3, 6, 10, −4	161, 50
19001	3, 6, 2, −10	149, 40	20929	5, 8, 8, −6	189, 86
19009	3, 10, 12, 0	253, 150	21001	11, 8, 2, −12	333, 212
19073	3, 12, 8, −2	221, 122	21017	5, 4, 2, 10	145, 2
19081	5, 0, 10, 4	141, 20	21089	11, 10, 4, 2	241, 136
19121	1, 14, 12, 6	377, 248	21121	3, 12, 0, −2	157, 42
19249	1, 10, 16, 6	393, 260	21169	9, 10, 4, 4	213, 110
19273	11, 8, 6, −8	285, 176	21193	7, 12, 2, 2	201, 98
19289	13, 14, 6, 0	401, 266	21313	3, 2, 12, 2	161, 48
19417	13, 8, 6, −2	273, 166	21377	11, 8, 8, 2	253, 146
19433	7, 6, 6, −8	185, 86	21401	3, 6, 2, 10	149, 20
19441	3, 4, 12, 8	233, 132	21433	13, 12, 2, −2	321, 202
19457	5, 2, 4, −10	145, 28	21481	15, 12, 6, −2	409, 270
19489	11, 0, 4, 2	141, 14	21521	9, 6, 4, −10	233, 128
19553	11, 8, 4, 2	205, 106	21529	5, 6, 10, −4	177, 70
19577	5, 10, 2, −8	193, 94	21569	5, 14, 8, −2	289, 176
19609	1, 12, 2, 0	149, 36	21577	15, 10, 6, −8	425, 282
19681	5, 0, 4, 10	141, 10	21601	1, 12, 12. 12	433, 288
19697	9, 8, 8, −6	245, 142	21617	7, 14, 4, −4	277, 166
19753	1, 6, 2, −10	141, 8	21649	7, 10, 12, 8	357, 230
19777	11, 6, 4, 2	177, 76	21673	1, 6, 14, 4	249, 142
19793	3, 12, 8, 8	281, 172	21713	13, 12, 0, −4	329, 208
19801	1, 12, 14, 4	357, 232	21737	3, 12, 2, −4	173, 64
19841	7, 8, 12, 0	257, 152	21817	5, 10, 2, 6	165, 52
19889	9. 2, 8, 0	149, 34	21841	11, 0, 4, 4	153, 28
19913	5, 8, 14, 4	301, 188	21881	11, 6, 6, 2	197, 92
19937	5, 14, 12, 0	365, 238	21929	9, 6, 10, 2	221, 116
19961	7, 4, 10, 4	181, 80	21937	1, 6, 8, 12	245, 138
19993	5, 12, 6, 6	241, 138	21961	9, 14, 2, −4	297, 182
20089	11, 0, 2, 6	161, 54	21977	11, 10, 10, −4	337, 214
20113	7, 6, 8, −6	185, 84	22073	7, 0, 6, 8	149, 8
20129	5, 12, 0, −2	173, 70	22129	7, 0, 8, 6	149, 6
20161	11, 12, 4, −10	381, 250	22153	11, 12, 10, 4	381, 248
20177	11, 4, 4, −8	217, 116	22193	9, 0, 8, 2	149, 2
20201	13, 4, 2, −8	253, 148	22273	5, 4, 12, 2	189, 82
20233	11, 4, 6, −4	189, 88	22369	13, 8, 0, −2	237, 130
20249	15, 12, 2, −4	389, 256	22409	5, 16, 10, 4	397, 260
20297	7, 10, 10, −4	265, 158	22433	5, 6, 12, 8	269, 158
20353	1, 12, 8, 0	209, 108	22441	1, 4, 6, −10	153, 22
20369	5, 8, 4, 8	169, 64	22481	1, 12, 12, 2	293, 178
20393	13, 4, 2, −4	205, 104	22697	7, 10, 10, 8	313, 194
20441	5, 10, 14, 10	421, 280	22721	9, 0, 4, 8	161, 40
20521	1, 12, 2, 2	153, 38	22769	15, 12, 8, −2	437, 290
20593	1, 6, 12, 0	181, 78	22777	5, 10, 6, 8	225, 118
20641	3, 14, 12, 2	353, 228	22817	5, 10, 4, −8	205, 98

Canonical prime factors. TAB. I. (*cont.*)

p	$a_0\ a_1\ a_2\ a_3$	$e\ \ f$	p	$a_0\ a_1\ a_2\ a_3$	$e\ \ f$
22921	5, 8, 6, −8	189, 80	23857	9, 10, 0, 2	185, 72
22937	1, 4, 14, 8	277, 164	23873	3, 6, 4, −10	161, 32
22961	1, 8, 4, 10	181, 70	23929	9, 16, 6, 0	373, 240
22993	1, 2, 4, 12	165, 46	23977	1, 10, 10, 12	345, 218
23017	7, 6, 2, 8	153, 14	23993	13, 12, 6, −10	449, 298
23041	5, 14, 8, 6	321, 200	24001	3, 0, 12, 2	157, 18
23057	9, 14, 8, −6	377, 244	24049	1, 0, 12, 6	181, 66
23081	7, 2, 10, −2	157, 28	24097	3, 10, 0, −8	173, 54
23201	3, 8, 8, −6	173, 58	24113	7, 6, 12, 4	245, 134
23209	1, 4, 10, −6	153, 10	24121	5, 0, 10, 6	161, 30
23297	5, 4, 4, 10	157, 26	24137	11, 4, 2, 4	157, 16
23321	1, 4, 6, 12	197, 88	24169	3, 8, 10, −4	189, 76
23369	15, 6, 2, −8	329, 206	24281	5, 10, 10, −4	241, 130
23417	3, 6, 14, 4	257, 146	24329	7, 2, 10, 4	169, 46
23473	7, 10, 4, 6	201, 92	24337	9, 2, 8, −4	165, 38
23497	9, 6, 2, 6	157, 24	24473	11, 4, 6, −6	209, 98
23537	7, 6, 12, 2	233, 124	24481	3, 10, 12, 12	397, 258
23561	1, 2, 10, −8	169, 50	24593	7, 8, 4, −10	229, 118
23593	3, 12, 6, −4	205, 96	24697	9, 4, 6, −8	197, 84
23609	11, 2, 6, 0	161, 34	24793	15, 8, 2, −4	309, 188
23633	11, 16, 4, −4	409, 268	24809	7, 10, 2, −10	253, 140
23689	11, 12, 2, 0	269, 156	24841	7, 14, 6, 4	297, 178
23753	9, 6, 10, −2	221, 112	24889	9, 12, 14, 0	421, 276
23761	9, 6, 8, −6	217, 108	24953	3, 2, 2, −12	161, 22
23801	13, 4, 2, −2	193, 82	24977	5, 4, 12, 0	185, 68
23833	11, 6, 2, −12	305, 186			

Simplest prime factors of $p = 16m + 1$. TABLE II.

See Table I. for any prime numbers not entered in this Table.

p	$a_0\ a_1\ a_2\ a_3$	p	$a_0\ a_1\ a_2\ a_3$	p	$a_0\ a_1\ a_2\ a_3$
113	1, 3, 0, 1	3169	3, 5, 2, 5	6737	7, 1, 2, −7
193	3, 1, 2, 1	3313	1, 3, 8, 1	6977	9, 1, 2, −3
353	1, 1, 4, −1	3457	1, 3, 2, 7	7057	5, 1, 6, 5
401	3, 1, 2, −3	3889	3, 1, 6, 5	7393	9, 3, 4, −3
673	3, 3, 2, 3	4001	3, 3, 8, 1	7457	5, 3, 6, −5
929	5, 1, 2, 1	4241	1, 5, 6, −3	7489	5, 3, 4, −7
1009	5, 1, 2, −3	4273	1, 7, 4, −3	7537	9, 1, 2, 1
1153	1, 3, 4, −3	4289	1, 5, 4, −5	7873	1, 9, 2, 3
1201	3, 3, 4, −3	4481	1, 1, 8, −1	8017	7, 3, 6, 3
1217	1, 5, 0, 3	4657	5, 3, 4, 5	8081	5, 1, 8, −1
1409	3, 3, 2, −5	4673	5, 1, 2, −7	8209	1, 9, 0, 3
1489	1, 3, 2, −5	5009	1, 3, 6, −5	8273	5, 1, 4, 7
1697	1, 3, 6, −1	5153	3, 9, 2, 1	8513	7, 1, 6, −3
1777	3, 5, 0, 3	5233	3, 1, 4, 7	8737	3, 1, 6, −7
1873	3, 3, 6, −1	5393	1, 5, 8, −1	8753	1, 1, 6, 9
2081	1, 1, 6, −3	5441	5, 5, 2, 5	8929	3, 3, 10, 3
2129	3, 3, 4, 5	5521	3, 5, 2, −7	9041	1, 7, 2, 7
2593	3, 1, 4, −5	5569	7, 5, 4, 3	9137	9, 3, 4, 1
2689	3, 7, 0, −3	5953	3, 3, 6, −5	9473	3, 7, 8, −3
2833	3, 7, 0, 1	6113	1, 5, 2, −7	9601	5, 7, 0, 5
2897	5, 1, 2, 5	6449	5, 9, 0, −1	9649	5, 3, 8, −3
3089	7, 3, 0, 1	6481	3, 9, 0, −1	9697	3, 9, 0, −5
3137	1, 1, 4, 7	6689	1, 9, 0, −1	9857	1, 1, 10, 5

Solutions of $x^2 + y^2 = n$. TABLE III.

n	x	y
1	1,	0
2	1,	1
4	2,	0
5	1,	2
8	2,	2
9	3,	0
10	3,	1
13	3,	2
16	4,	0
17	1,	4
18	3,	3
20	4,	2
25	5,	0
	3,	4
26	5,	1
29	5,	2
32	4,	4
34	5,	3
36	6,	0
37	1,	6
40	6,	2
41	5,	4
45	3,	6
49	7,	0
50	5,	5
	7,	1
52	6,	4
53	7,	2
58	7,	3
61	5,	6
64	8,	0
65	7,	4
	1,	8
68	8,	2
72	6,	6
73	3,	8
74	7,	5
80	8,	4
81	9,	0
82	9,	1
85	9,	2
	7,	6
89	5,	8
90	9,	3
97	9,	4
98	7,	7
100	10,	0
	8,	6
101	1,	10
104	10,	2
106	9,	5
109	3,	10
113	7,	8

n	x	y
116	10,	4
117	9,	6
121	11,	0
122	11,	1
125	5,	10
	11,	2
128	8,	8
130	11,	3
	9,	7
136	10,	6
137	11,	4
144	12,	0
145	9,	8
	1,	12
146	11,	5
148	12,	2
149	7,	10
153	3,	12
157	11,	6
160	12,	4
162	9,	9
164	10,	8
169	13,	0
	5,	12
170	13,	1
	11,	7
173	13,	2
178	13,	3
180	12,	6
181	9,	10
185	13,	4
	11,	8
193	7,	12
194	13,	5
196	14,	0
197	1,	14
200	10,	10
	14,	2
202	11,	9
205	13,	6
	3,	14
208	12,	8
212	14,	4
218	13,	7
221	11,	10
	5,	14
225	15,	0
	9,	12
226	15,	1
229	15,	2
232	14,	6
233	13,	8
234	15,	3

n	x	y
241	15,	4
242	11,	11
244	12,	10
245	7,	14
250	15,	5
	13,	9
256	16,	0
257	1,	16
260	14,	8
	16,	2
261	15,	6
265	11,	12
	3,	16
269	13,	10
272	16,	4
274	15,	7
277	9,	14
281	5,	16
288	12,	12
289	17,	0
	15,	8
290	17,	1
	13,	11
292	16,	6
293	17,	2
296	14,	10
298	17,	3
305	17,	4
	7,	16
306	15,	9
313	13,	12
314	17,	5
317	11,	14
320	16,	8
324	18,	0
325	17,	6
	15,	10
	1,	18
328	18,	2
333	3,	18
337	9,	16
338	17,	7
	13,	13
340	18,	4
	14,	12
346	15,	11
349	5,	18
353	17,	8
356	16,	10
360	18,	6
361	19,	0
362	19,	1

n	x	y
365	19,	2
	13,	14
369	15,	12
370	19,	3
	17,	9
373	7,	18
377	19,	4
	11,	16
386	19,	5
388	18,	8
389	17,	10
392	14,	14
394	15,	13
397	19,	6
400	20,	0
	16,	12
401	1,	20
404	20,	2
405	9,	18
409	3,	20
410	19,	7
	17,	11
416	20,	4
421	15,	14
424	18,	10
425	19,	8
	13,	16
	5,	20
433	17,	12
436	20,	6
441	21,	0
442	21,	1
	19,	9
445	21,	2
	11,	18
449	7,	20
450	21,	3
	15,	15
452	16,	14
457	21,	4
458	17,	13
461	19,	10
464	20,	8
466	21,	5
468	18,	12
477	21,	6
481	15,	16
	9,	20
482	19,	11
484	22,	0
485	17,	14
	1,	22
488	22,	2

Solutions of $x^2+y^2=n$. TAB. III. (*cont.*)

n	x	y
490	21,	7
493	13,	18
	3,	22
500	22,	4
	20,	10
505	21,	8
	19,	12
509	5,	22
512	16,	16
514	17,	15
520	22,	6
	18,	14
521	11,	20
522	21,	9
529	23,	0
530	23,	1
	19,	13
533	23,	2
	7,	22
538	23,	3
541	21,	10
544	20,	12
545	23,	4
	17,	16
548	22,	8
549	15,	18
554	23,	5
557	19,	14
562	21,	11
565	23,	6
	9,	22
569	13,	20
576	24,	0
577	1,	24
578	23,	7
	17,	17
580	24,	2
	18,	16
584	22,	10
585	21,	12
	3,	24
586	19,	15
592	24,	4
593	23,	8
596	20,	14
601	5,	24
605	11,	22
610	23,	9
	21,	13
612	24,	6
613	17,	18
617	19,	16

n	x	y
625	25,	0
	15,	20
	7,	24
626	25,	1
628	22,	12
629	25,	2
	23,	10
634	25,	3
637	21,	14
640	24,	8
641	25,	4
648	18,	18
650	25,	5
	23,	11
	19,	17
653	13,	22
656	20,	16
657	9,	24
661	25,	6
666	21,	15
673	23,	12
674	25,	7
676	26,	0
	24,	10
677	1,	26
680	26,	2
	22,	14
685	19,	18
	3,	26
689	25,	8
	17,	20
692	26,	4
697	21,	16
	11,	24
698	23,	13
701	5,	26
706	25,	9
709	15,	22
712	26,	6
720	24,	12
722	19,	19
724	20,	18
725	25,	10
	23,	14
	7,	26
729	27,	0
730	27,	1
	21,	17
733	27,	2
738	27,	3
740	26,	8
	22,	16

n	x	y
745	27,	4
	13,	24
746	25,	11
754	27,	5
	23,	15
757	9,	26
761	19,	20
765	27,	6
	21,	18
769	25,	12
772	24,	14
773	17,	22
776	26,	10
778	27,	7
784	28,	0
785	23,	16
	1,	28
788	28,	2
793	27,	8
	3,	28
794	25,	13
797	11,	26
800	28,	4
	20,	20
801	15,	24
802	21,	19
808	22,	18
809	5,	28
810	27,	9
818	23,	17
820	28,	6
	26,	12
821	25,	14
829	27,	10
832	24,	16
833	7,	28
841	29,	0
	21,	20
842	29,	1
845	29,	2
	19,	22
	13,	26
848	28,	8
850	29,	3
	27,	11
	25,	15
853	23,	18
857	29,	4
865	17,	24
	9,	28
866	29,	5
872	26,	14

n	x	y
873	27,	12
877	29,	6
881	25,	16
882	21,	21
884	28,	10
	22,	20
890	29,	7
	23,	19
898	27,	13
900	30,	0
	24,	18
901	15,	26
	1,	30
904	30,	2
905	29,	8
	11,	28
909	3,	30
914	25,	17
916	30,	4
922	29,	9
925	27,	14
	21,	22
	5,	30
928	28,	12
929	23,	20
932	26,	16
936	30,	6
937	19,	24
941	29,	10
949	25,	18
	7,	30
953	13,	28
954	27,	15
961	31,	0
962	31,	1
	29,	11
964	30,	8
965	31,	2
	17,	26
968	22,	22
970	31,	3
	23,	21
976	24,	20
977	31,	4
980	28,	14
981	9,	30
985	29,	12
	27,	16
986	31,	5
	25,	19
997	31,	6
1000	30,	10
	26,	18

ON THE LAW OF QUARTIC RECIPROCITY.

By *Thorold Gosset.*

THE law of quartic reciprocity, applicable to real primes, discovered and proved by Gauss, may be stated in the following manner:—

Let p be a real prime of the form $4n+1$, and therefore equal to a^2+b^2, where a is a real odd number and b a real even number. Then, if q is a real prime of the form $4n+1$,

$$\left(\frac{q}{a+bi}\right)_4 = 1,\ -1,\ i,\ \text{or}\ -i,$$

accordingly as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1,\ -1,\ i,\ \text{or}\ -i \pmod{q},$$

and if q is a real prime of the form $4n-1$

$$\left(\frac{-q}{a+bi}\right)_4 = 1,\ -1,\ i,\ \text{or}\ -i,$$

accordingly as

$$\left(\frac{a-bi}{a+bi}\right)^{\frac{1}{4}(q+1)} \equiv 1,\ -1,\ i,\ \text{or}\ -i \pmod{q}.$$

Since $q^{\frac{1}{4}(p-1)} \equiv 1,\ -1,\ a/b$, or $-a/b \pmod{p}$, we shall signify by the notation $(q/p)_4$ that one of the above four values to which $q^{\frac{1}{4}(p-1)}$ is congruent $(\text{mod}\, p)$.

It is evident that the value of $(q/p)_4$ can always theoretically be found from Gauss' formulæ; but, when q is not a very small number, the imaginary quantities make the calculation extremely troublesome.

When p and q are given, finding the actual value $(q/p)_4$ is a problem which apparently only involves real quantities, and it would therefore seem to be theoretically possible to eliminate the imaginary quantities from the formulæ.

We proceed to show how this may be done. In the first place, suppose q a prime of the form $4n+1$, and let $q=\alpha^2+\beta^2$.

Since $(\alpha+\beta i)$ and $(\alpha-\beta i)$ are factors of q,

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1,\ -1,\ i,\ \text{or}\ -i \pmod{\alpha-\beta i},$$

accordingly as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1,\ -1,\ i,\ \text{or}\ -i \pmod{q}.$$

Taking the reciprocals on each side of the first congruence

$$\left(\frac{a-bi}{a+bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, -i, \text{ or } i \pmod{\alpha-\beta i},$$

accordingly as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, i, \text{ or } -i \pmod{q}.$$

But $i \equiv \alpha/\beta \pmod{\alpha-\beta i}$; therefore

$$\left(\frac{a/b-\alpha/\beta}{a/b+\alpha/\beta}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, -\alpha/\beta, \text{ or } \alpha/\beta \pmod{\alpha-\beta i},$$

accordingly as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, i, \text{ or } -i \pmod{q} \ldots\ldots(1).$$

Again as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, i, \text{ or } -i \pmod{\alpha+\beta i},$$

accordingly as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, i, \text{ or } -i \pmod{q},$$

and $i \equiv -\alpha/\beta \pmod{\alpha+\beta i}$. Therefore

$$\left(\frac{a/b-\alpha/\beta}{a/b+\alpha/\beta}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, -\alpha/\beta, \text{ or } \alpha/\beta \pmod{\alpha+\beta i},$$

accordingly as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, i, \text{ or } -i \pmod{q} \ldots\ldots(2).$$

Hence $\left(\frac{a/b-\alpha/\beta}{a/b+\alpha/\beta}\right)^{\frac{1}{4}(q-1)}$ is congruent to precisely the same real number, no matter whether the modulus be $\alpha+\beta i$ or $\alpha-\beta i$, and will therefore be congruent to the same number $\pmod{q}$ so that

$$\left(\frac{a/b-\alpha/\beta}{a/b+\alpha/\beta}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, -\alpha/\beta, \text{ or } \alpha/\beta \pmod{q},$$

accordingly as

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, i, \text{ or } -i \pmod{q} \ldots\ldots(3).$$

Again, since $\left(\dfrac{q}{a+bi}\right)_4 \equiv q^{\frac{1}{4}(p-1)} \pmod{a+bi}$,

we have, accordingly as $\left(\dfrac{q}{a+bi}\right)_4 = 1, -1, i,$ or $-i$,

$$q^{\frac{1}{4}(p-1)} \text{ congruent to } 1, -1, i, \text{ or } -i \pmod{a+bi}$$

or to $$1, -1, -\frac{a}{b}, \text{ or } \frac{a}{b} \pmod{a+bi} \ldots\ldots\ldots\ldots(4).$$

But, accordingly as

$$q^{\frac{1}{4}(p-1)} \text{ is congruent to } 1, -1, i, \text{ or } -i \pmod{a+bi},$$

$$q^{\frac{1}{4}(p-1)} \text{ is congruent to } 1, -1, -i, \text{ or } i \pmod{a-bi},$$

for it is indifferent which root of -1 we use, and consequently, accordingly as $\left(\dfrac{q}{a+bi}\right)_4 = 1, -1, i,$ or $-i$,

$$q^{\frac{1}{4}(p-1)} \text{ is congruent } 1, -1, -\frac{a}{b}, \text{ or } \frac{a}{b} \pmod{a-bi} \ldots(5).$$

Here again $q^{\frac{1}{4}(p-1)}$ is congruent to precisely the same real number, whether the modulus be $(a+bi)$ or $(a-bi)$, and is therefore congruent to the same number $(\text{mod}\, p)$. Therefore $(q/p)_4 = 1, -1, -a/b$ or a/b, accordingly as

$$\left(\frac{q}{a+bi}\right)_4 = 1, -1, i, \text{ or } -i \ldots\ldots\ldots\ldots\ldots(6).$$

Combining the results in (3) and (6) with the original statement of the law of quartic reciprocity, we have

$$\left(\frac{q}{p}\right)_4 = 1, \ -1, \ -\frac{a}{b}, \text{ or } \frac{a}{b},$$

accordingly as

$$\left(\frac{a/b - \alpha/\beta}{a/b + \alpha/\beta}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, -\alpha/\beta, \text{ or } \alpha/\beta \pmod{q} \ldots(7).$$

In (7) no imaginary quantities appear at all. If q is a prime of the form $4n+1$ less than 1000, Jacobi's *Canon Arithmeticus* can be used to rapidly find the value of

$$\left(\frac{a/b - \alpha/\beta}{a/b + \alpha/\beta}\right)^{\frac{1}{4}(q-1)} \pmod{q}.$$

Cunningham's *Quadratic Partitions* can be used to find the values of a, b or α, β when p or q is less than 100,000. It may be remarked that no convention is necessary as to the sign of a, b, α, or β, and that there is no occasion to find the values of α and β if we have the solution of $x^2 \equiv -1 \pmod q$, for, if $x^2 \equiv -1 \pmod q$, $x = \pm \alpha/\beta$, and consequently either value of x may be written in formula (7) in the place of α/β.

The above method only applies when q is a prime of the form $4n+1$, but, when q is of the form $4n-1$, we can usually find a number having the same residuacity as q composed exclusively of primes of the form $4n+1$ that are within the limits of Jacobi's tables; for instance, if we wanted to find $\left(\frac{223}{3137}\right)_4$, we have

$$223 \equiv 223 + 2 \,.\, 3137 \equiv 6497 \equiv 73 \times 89 \pmod{3137},$$

and the formula can be applied in turn to 73 and 89 instead of 223.

We now give another method of eliminating imaginaries that can be applied, whether q be of the form $4n+1$ or $4n-1$.

Let $a = r\cos\theta$ and $b = r\sin\theta$, so that $b/a = \tan\theta$. We write n for the nearest integer to $\frac{1}{4}q$ so that $n = \frac{1}{4}(q-1)$ or $\frac{1}{4}(q+1)$, accordingly as q is of the form $4n+1$ or $4n-1$. Then

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} = \left(\frac{r\cos\theta + ir\sin\theta}{r\cos\theta - ir\sin\theta}\right)^n = \frac{(\cos\theta + i\sin\theta)^n}{(\cos\theta - i\sin\theta)^n}$$

$$= \frac{\cos n\theta + i\sin n\theta}{\cos n\theta - i\sin n\theta} = \frac{1 + i\tan n\theta}{1 - i\tan n\theta}.$$

Consequently

$$\left(\frac{a+bi}{a-bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, -1, i, \text{ or } -i \pmod q,$$

accordingly as

$$\tan n\theta \equiv 0, \infty, 1, \text{ or } -1 \pmod q.$$

The meaning of $\tan n\theta \equiv \infty \pmod q$ is simply that the denominator of $\tan n\theta$ is divisible by q. In this case we have

$$\frac{\cos n\theta + i\sin n\theta}{\cos n\theta - i\sin n\theta} \equiv -1 \pmod q,$$

from which we deduce

$$\cos n\theta \equiv 0 \pmod q.$$

We shall continue to employ the congruence $x \equiv \infty \pmod{q}$ to denote the case where x is a fraction, which, when reduced to its lowest terms, has a denominator divisible by q. When q is of the form $4n-1$, we have, in a precisely similar manner,

$$\left(\frac{a-bi}{a+bi}\right)^{\frac{1}{4}(q-1)} \equiv 1, \ -1, \ i, \text{ or } -i,$$

accordingly as

$$\tan n\theta \equiv 0, \ \infty, \ -1, \text{ or } 1 \pmod{q}.$$

Hence we may state Gauss' law as follows:—

Let $\tan\theta = b/a$. When q is of the form $4n+1$; then

$$\left(\frac{q}{p}\right)_4 = 1, \ -1, \ \frac{a}{b}, \text{ or } -\frac{a}{b},$$

accordingly as

$$\tan n\theta = 0, \ \infty, \ -1, \text{ or } 1 \pmod{q} \text{..........(8)}.$$

When q is of the form $4n-1$; then

$$\left(\frac{-q}{p}\right)_4 = 1, \ -1, \ \frac{a}{b}, \text{ or } -\frac{a}{b},$$

accordingly as

$$\tan n\theta \equiv 0, \ \infty, \ 1, \text{ or } -1 \pmod{q} \text{..........(9)}.$$

To show that this formula can be practically applied without much labour, we use it to find $\left(\frac{67}{99989}\right)_4$. Here $67 = 4.17 - 1$; therefore $n = 17$.

From Cunningham's tables $99989 = 217^2 + 230^2$. Therefore

$$\tan\theta \equiv \frac{230}{217} \equiv \frac{29}{16} \equiv \frac{96}{16} \equiv 6 \pmod{67},$$

$$\tan 2\theta \equiv \frac{2.6}{1-6^2} \equiv \frac{12}{-35} \equiv \frac{-24}{70} \equiv \frac{-24}{3} \equiv -8 \pmod{67},$$

$$\tan 4\theta \equiv \frac{-2.8}{1-8^2} \equiv \frac{-16}{-63} \equiv \frac{-16}{4} \equiv -4 \pmod{67},$$

$$\tan 8\theta \equiv \frac{-2.4}{1-4^2} \equiv \frac{-8}{-15} \equiv \frac{-32}{-60} \equiv \frac{35}{7} \equiv 5 \pmod{67},$$

$$\tan 16\theta \equiv \frac{2.5}{1-5^2} \equiv \frac{10}{-24} \equiv \frac{-5}{12} \equiv \frac{-72}{12} \equiv -6 \pmod{67},$$

$$\tan 17\theta = \tan(\theta + 16\theta) \equiv \frac{6-6}{1+6^2} \equiv \frac{0}{37} \equiv 0 \pmod{67}.$$

Therefore $\left(\frac{-67}{99989}\right)_4 = 1$, and, since 99989 is of the form $8m+5$, $\left(\frac{-1}{99989}\right)_4 = -1$; consequently $\left(\frac{67}{99989}\right)_4 = -1$.

The fact that $\tan n\theta$ must have one of the four values $0, \infty, \pm 1 \pmod q$ is a useful check on the acccuracy of the work, and even as it stands the amount of work involved by the use of tangents is not excessive. We shall show later however, that it might have been considerably shortened.

As similar considerations apply to the laws of cubic and octavic reciprocity, we will now investigate the properties of $\tan r\theta \pmod q$. Consider the series

$$\tan 0,\ \tan\theta,\ \tan 2\theta,\ \tan 3\theta,\ \text{etc.},$$

in which $\tan\theta$ is a commensurable number. It follows from the ordinary formulæ for addition of tangents that $\tan r\theta$ must also be commensurable; consequently every term in the series must be congruent to one of the following $(q+1)$ numbers $(\text{mod}\, q)$:

$$0,\ 1,\ 2,\ 3,\ \ldots,\ (q-2),\ (q-1),\ \infty,$$

so that, after taking $(q+2)$ terms, at least two terms must be congruent to one another.

Let $\tan k\theta \equiv \tan l\theta \pmod q$. Then, since

$$\tan k\theta - \tan l\theta = \tan (k-l)\,\theta\,\{1 + \tan k\theta . \tan l\theta\},$$

it follows that unless $1 + \tan k\theta . \tan l\theta \equiv 0 \pmod q$

$$\tan (k-l)\,\theta \equiv 0 \pmod q.$$

By supposing $\tan k\theta = t/q^m$ and $\tan l\theta = t'/q^{m'}$, we have

$$\tan (k-l)\,\theta = \frac{t/q^m - t'/q^{m'}}{1 + tt'/q^{m+m'}} = \frac{q^{m'}t - q^m t'}{q^{m+m'} + tt'} \equiv \frac{q^{m'}t - q^m t'}{tt'} \equiv 0 \pmod q.$$

Consequently $\tan k\theta \equiv \tan l\theta \equiv \infty \pmod q$ is no exception to the rule.

If $$1 + \tan k\theta . \tan l\theta \equiv 0 \pmod q,$$

and $$\tan k\theta \equiv \tan l\theta \pmod q,$$

we have $$1 + \tan^2 k\theta \equiv 0 \pmod q.$$

In this case, if $\tan\phi \not\equiv -\tan k\theta \pmod q$,

$$\tan(k\theta+\phi) = \frac{\tan k\theta + \tan\phi}{1-\tan k\theta . \tan\phi}$$

$$= \frac{\tan k\theta\,(\tan k\theta+\tan\phi)}{\tan k\theta + \tan\phi - \tan\phi\,(1+\tan^2 k\theta)} \equiv \tan k\theta \pmod q.$$

Consequently in this case all the terms in the series (except the initial 0) are congruent to the same number $\pmod q$. If

$$1+\tan^2\theta \equiv 0 \pmod q,$$

$1+b^2/a^2$, and therefore $a^2+b^2\equiv 0 \pmod q$, so in this case p is a multiple of q, and this involves, if q and p are both primes, $p=q$. We shall accordingly assume that $\tan\theta$ does not satisfy the congruence $1+\tan^2\theta\equiv 0 \pmod q$.

When q is of the form $4n-1$, there can be no solution to this congruence, but when q is of the form $4n+1$ there are always two solutions. Both these are thus excluded from the series, so that, whether q is of the form $4n+1$ or $4n-1$, the maximum number of terms in the series, no two of which are congruent one to another, is $4n$.

Suppose f is the least multiple of θ, for which $\tan f\theta \equiv 0 \pmod q$. Then we may say f is the multiple of θ to which $\tan\theta$ appertains. The quantities

$$\tan 0,\ \tan\theta,\ \tan 2\theta,\ \ldots,\ \tan(f-1)\,\theta$$

are all incongruent, for, if $\tan k\theta \equiv \tan l\theta \pmod q$, where k and l are less than f, we have $\tan(k-l)\,\theta\equiv 0 \pmod q$, which is contrary to the definition of f. If $k\equiv l \pmod f$, we have $\tan k\theta \equiv \tan l\theta \pmod q$, so that the terms recur periodically after the first f terms. If f is less than $4n$, there will be at least one residue, say $\tan\phi$, which does not occur in the period and does not satisfy the congruence

$$1+\tan^2\phi\equiv 0 \pmod q.$$

Then none of the terms in the series

$$\tan\phi,\ \tan(\phi+\theta),\ \ldots,\ \tan\{\phi+(f-1)\}\,\theta$$

can be congruent to any of the terms of the first series or to one another, for, if $\tan(\phi+k\theta)\equiv\tan l\theta$,

$$\tan\{\phi+(k-l)\,\theta\}\equiv 0 \pmod q$$

and

$$\tan\phi\equiv\tan(l-k)\,\theta,$$

or $\tan(f+l-k)\,\theta$, accordingly as l is greater or less than k.

Similarly, if there still remain any of the $4n$ terms, which have not been included in either of the series, we may take another series $\tan\psi$, $\tan(\psi+\theta)$, ..., $\tan\{\psi+(f-1)\}\theta$, and show that every term in this series is incongruent to every term in the previous two series.

This process can be continued indefinitely till all the residues are exhausted, except the two residues which satisfy $x^2+1\equiv 0 \pmod{q}$ when q is the form $4n+1$. Consequently f is always a divisor of $4n$.

Since

$$\tan f\theta = \frac{f\tan\theta - \{f(f-1)(f-2)/3!\}\tan^3\theta + \dots}{1-\{f(f-1)/2!\}\tan^2\theta + \dots},$$

$\tan f\theta$ may be congruent to 0 $(\mathrm{mod}\, q)$ either through the numerator being congruent to 0 or the denominator being congruent to ∞. The latter can only occur when $\tan\theta\equiv\infty$ $(\mathrm{mod}\, q)$, and the denominator contains $\tan\theta$ to a higher power than the numerator. This will be the case when f is even, for then the highest power of $\tan\theta$ in the numerator is $\tan^{f-1}\theta$ and the highest power in the denominator is $\tan^f\theta$; there will consequently be one infinite solution and not more than $f-1$ finite solutions to the congruence $\tan f\theta\equiv 0 \pmod{q}$. When f is odd the highest power of $\tan\theta$ in the numerator is $\tan^f\theta$, and in the denominator $\tan^{f-1}\theta$, so that in this case there are not more than f finite solutions and no infinite solutions.

If a residue $\tan\theta$ can be found appertaining to the multiple f of θ, then the f quantities $\tan\theta$, $\tan 2\theta$, ..., $\tan f\theta$ are all roots of the congruence $\tan f\theta\equiv 0 \pmod{q}$; and as there are only f roots of this congruence they are all the roots. Of these f roots (if they exist), there will be a certain number which appertain to a smaller multiple of θ than f, thus if k be a divisor of f, $\tan k\theta$ will appertain to the multiple f/k, so that the total number of roots appertaining to the multiple f will be the number of numbers less than f and prime to it (including unity), *i.e.*, $\phi(f)$ or else zero, for we have only proceeded on the supposition that some residue appertaining to the multiple of f can be found.

But every residue [except the two which satisfy $x^2+1=0$ $(\mathrm{mod}\, q)$ when q is of the form $4n+1$] appertains to some multiple, and this multiple is a divisor of $4n$, so that the total number of residues appertaining to all the divisors of $4n$ must be $4n$, and if f_1, f_2, f_3 be the different divisors of $4n$ we have

the well-known relation

$$\phi(f_1) + \phi(f_2) + \phi(f_3) + \ldots = 4n,$$

so that it is not possible for the number of residues appertaining to the multiple f to be zero if f is a divisor of $4n$. There are therefore $\phi(f)$ residues appertaining to the multiple f, and in particular $\phi(4n)$ residues appertaining to the multiple $4n$. We may call these latter primitive tangent roots of q.

The whole theory of tangent residues is practically identical with that of the ordinary power residues. Starting with any primitive tangent root $\tan\theta$, we may obtain successively the $4n$ residues. These will include the two values 0 and ∞, which do not occur in the power residues, and when $q = 4n+1$ will exclude the two solutions of $x^2 + 1 = 0 \pmod{q}$, which do occur in the power residues.

Corresponding to Fermat's theorem we have the result, when q is prime, $\tan 4n\theta$ is necessarily divisible by q.

To illustrate the relationship of the tangent residues, I give a table of them for the prime 79, constructed upon similar principles to those adopted for power residues in Jacobi's *Canon Arithmeticus* and Cunningham's *Binary Canon*. The first table gives the residues for successive multiples of θ, starting with $\tan\theta = 6$: 6 will be seen to be the smallest primitive tangent root of 79. The second table gives the multiple of θ which corresponds to a given residue. The values in the first table are obtained successsively from the relation $\tan(r+1)\theta \equiv \dfrac{6+\tan r\theta}{1-6\tan r\theta} \pmod{79}$. Those in the second table are merely obtained by inverting the values in the first table.

TABLE I. *Residues in terms of Multiples* $(q = 79)$.

Multiples	0	1	2	3	4	5	6	7	8	9
–	0	6	29	24	2	28	5	65	25	21
1	8	35	72	11	52	59	26	37	57	67
2	1	46	61	47	76	75	38	36	45	70
3	10	64	19	62	16	48	40	56	30	66
4	∞	13	49	23	39	31	63	17	60	15
5	69	9	34	43	41	4	3	32	18	33
6	78	12	22	42	53	20	27	68	7	44
7	71	58	54	14	74	51	77	55	50	73
8	0	..	..	..	..	..	..	..	..	..

TABLE II. *Multiples in terms of Residues* ($q=79$).

Residues	0	1	2	3	4	5	6	7	8	9
–	80	20	4	56	55	6	1	68	10	51
1	30	13	61	41	73	49	34	47	58	32
2	65	9	62	43	3	8	16	66	5	2
3	38	45	57	59	52	11	27	17	26	44
4	36	54	63	53	69	28	21	23	35	42
5	78	75	14	64	72	77	37	18	71	15
6	48	22	33	46	31	7	39	19	67	50
7	29	70	12	79	74	25	24	76	60	..
∞	40	..	..	..	..	..	..	..	..	..

We see from either table

$$\tan 20\theta \equiv 1 \equiv \tan \tfrac{1}{4}\pi \quad (\text{mod } 79),$$

$$\tan 40\theta \equiv \infty \equiv \tan \tfrac{1}{2}\pi \quad (\text{mod } 79),$$

$$\tan 60\theta \equiv -1 \equiv \tan \tfrac{3}{4}\pi \quad (\text{mod } 79),$$

$$\tan 80\theta \equiv 0 \equiv \tan \pi \quad (\text{mod } 79).$$

With suitable conventions as to the signs of square roots, there is no difficulty in extending the process. Thus $9^2 \equiv 2$ (mod 79), and if we treat 9 as the positive square root of 2 (mod 79), we have

$$\tan 10\theta \equiv 8 \equiv \sqrt{2}-1 \equiv \tan \tfrac{1}{8}\pi \quad (\text{mod } 79),$$

$$\tan 30\theta = 10 \equiv \sqrt{2}+1 \equiv \tan \tfrac{3}{8}\pi \quad (\text{mod } 79),$$

$$\tan 50\theta = 69 \equiv -\sqrt{2}-1 \equiv \tan \tfrac{5}{8}\pi \quad (\text{mod } 79),$$

$$\tan 70\theta = 71 \equiv -\sqrt{2}+1 \equiv \tan \tfrac{7}{8}\pi \quad (\text{mod } 79).$$

Similarly $20^2 \equiv 5$ (mod 79) and $26^2 \equiv 44$ (mod 79), and if we treat 20 and 26 as the positive square roots of 5 and 44 (mod 79), we have

$$\tan 16\theta \equiv 26 \equiv \sqrt{44} \equiv \sqrt{(5+39)} \equiv \sqrt{(5-40)}$$

$$\equiv \sqrt{(5-2\times 20)} \equiv \sqrt{(5-2\sqrt{5})} \equiv \tan \tfrac{1}{5}\pi \quad (\text{mod } 79).$$

[It may be remarked that, although, for instance, $9^2 \equiv 2$ (mod 79), it is not strictly correct, except in accordance with a convention, to write either $9 \equiv \sqrt{2}$ (mod 79) or $9 \equiv -\sqrt{2}$ (mod 79), for 79 may be regarded as composed of two factors $9-\sqrt{2}$ and $9+\sqrt{2}$, and we have strictly $9 \equiv \sqrt{2}$ $\{\text{mod } (9-\sqrt{2})\}$ and $9 \equiv -\sqrt{2}$ $\{\text{mod } (9+\sqrt{2})\}$, but neither $9 \equiv \sqrt{2}$ or $9 \equiv -\sqrt{2}$ can be true for the product of the moduli, so that, adopting

the convention, $9 \equiv \sqrt{2} \pmod{79}$ is in reality equivalent to writing 79 in the place of its incommensurable factor $9 - \sqrt{2}$. Similarly $20 \equiv \sqrt{5} \pmod{79}$ would be more correctly written $20 \equiv \sqrt{5}\ \{\bmod (4\sqrt{5} - 1)\}$ and $26 = \sqrt{44} \pmod{79}$ would be more correctly written $26 \equiv \sqrt{44}\ \{\bmod (5\sqrt{11} + 14)\}$.]

All the trigonometrical relations, which hold between the tangents or inverse tangents of different angles, will be true of the residues and multiples shown in the above tables; for instance, the identity

$$\tan^{-1} 2 + \tan^{-1} 5 + \tan^{-1} 8 = \tan^{-1} 1$$

gives

$$4\theta + 6\theta + 10\theta = 20\theta$$

and

$$\tan^{-1} 2 + \tan^{-1} 3 = \tan^{-1} - 1$$

gives

$$4\theta + 56\theta = 60\theta.$$

The method of using Table II. to find the quartic residuacity of -79 may be illustrated by an example. From (9) above, we have

$$\left(\frac{-79}{p}\right)_4 = 1,\ -1,\ \frac{a}{b},\ \text{or}\ -\frac{a}{b},$$

accordingly as

$$\tan 20\theta' \equiv 0,\ \infty,\ 1,\ \text{or} -1 \pmod{79},$$

where $\tan\theta'$ stands for b/a, and $p = a^2 + b^2$; and

$$\tan 20\theta' = 0,\ \infty,\ 1,\ \text{or} -1,$$

accordingly as θ' is of the form $4m\theta$, $(4m+2)\,\theta$, $(4m+1)\,\theta$, or $(4m+3)\,\theta$, where $\tan\theta \equiv 6 \pmod{79}$; so that

$$\left(\frac{-79}{p}\right)_4 = 1,\ -1,\ \frac{a}{b},\ -\frac{a}{b},$$

accordingly as θ' is of the form $4m\theta$, $(4m+2)\,\theta$, $(4m+1)\,\theta$, or $(4m+3)\,\theta$.

If p, for instance, be $8122369 = 1537^2 + 2400^2$,

$$\tan\theta' \equiv \frac{2400}{1537} \equiv \frac{30}{36} \equiv \frac{5}{6} \equiv \frac{84}{6} \equiv 14 \equiv \tan 73\theta$$

and

$$73 = 4m + 1.$$

Hence

$$\left(\frac{-79}{p}\right)_4 = \frac{a}{b}.$$

Since p, in this case, is of the form $8r + 1$,

$$\left(\frac{79}{p}\right)_4 = \left(\frac{-79}{p}\right)_4.$$

If we have tables of the multiples of θ, for the prime of which the residuacity is to be determined, the residuacity can thus be practically read off provided we can effect the partition of p into the form a^2+b^2.

The principal object of the tables is to ascertain whether the given value of t in the congruence $\tan\theta' \equiv \tan t\theta \pmod q$ is of the form $4m$, $4m+1$, $4m+2$, $4m+3$; or, as we may shortly put it, what quartic character is indicated by $\tan\theta'$.

We now proceed to show that the quartic character of q, indicated by any particular value of $\tan\theta'$, depends merely on the linear form of q.

In the first instance, we may take a few simple forms of $\tan\theta$ and show, with such values for $\tan\theta$, the quartic residuacity of q can be completely determined without tables, no matter what the magnitude of q may be. To avoid distinguishing the cases, we shall suppose q to be of the form $4n+1$, so that if we are dealing with a number of the form $4n'-1=q'$, say, we suppose $q=-q'$, n will then equal $-n'$.

1. If $\tan\theta' \equiv 0$; that is to say, if b be divisible by q. Here $t=4n$, so that q is always a quartic residue. This is true for composite as well as prime values of q, as any composite value of q, if of the form $4n+1$, can be regarded as composed exclusively of primes, positive or negative, of the form $4n+1$. Thus we need not use the table to see that -79 is a quartic residue of $8753153=1537^2+2528^2$, since $2528=32\times 79$.

2. If $\tan\theta' \equiv \infty$; that is to say, if a be divisible by q. Here $t=2n$, so that $(q/p)_4=1$ or -1 accordingly as n is even or odd; that is to say, accordingly as q is of the form $8r+1$ or $8r+5$. As a composite number is of the form $8r+1$ or $8r+5$ accordingly as there are an even or odd number of primes of the form $8r+5$ composing it, this is true for composite numbers as well as primes. Thus if

$$p=7114753=897^2+2512^2,$$

$$\left(\frac{897}{p}\right)_4=1,$$

897 being of the form $8r+1$ and, of course, being a divisor of 897. We regard 897 as being composed of

$$-3\times 13\times -23,$$

all primes of the form $4n+1$.

3. If $\tan\theta' \equiv 1$; that is to say, if $a-b$ is divisible by q. Here $t=n$ or $3n$ according to the primitive tangent root chosen. We may suppose it chosen so that $t=3n$ when q is of the form $4n+1$, and $t=n'$ when q is of the form $4n'-1$, so that in every case $t=3n$, for $\tan 3n\theta$ is always congruent to $\tan -n\theta$ or $\tan n'\theta$. This convention is, of course, quite unnecessary and is merely adopted to avoid considering the two cases and to make the quartic character indicated by $\tan(4m+1)\theta$, a/b and by $\tan(4m+3)\theta$, $-a/b$, as in the particular tables given above relating to the quartic character of -79.

Now, accordingly as q is of the form $16r+1$, $16r+5$, $16r+9$, $16r+13$, n is of the form $4r$, $4r+1$, $4r+2$, $4r+3$, and $3n$ is of the form $4r$, $4r+3$, $4r+2$, $4r+1$, and accordingly $(q/p)_4$ is equal to 1, $-a/b$, -1, a/b, so that we have, when $a\equiv b \pmod q$,

$$\left(\frac{q}{p}\right)_4 = 1,\ -\frac{a}{b},\ -1,\ \text{or}\ \frac{a}{b},$$

accordingly as q is of the form $16r+1$, $16r+5$, $16r+9$, or $16r+13$. For instance

$$\left(\frac{13}{769}\right)_4 = \frac{a}{b}\ \text{ or }\ \frac{25}{12},$$

since $769 = 25^2+12^2$ and $25 \equiv 12 \pmod{13}$,

$$\frac{25}{12} \equiv -\frac{769-25}{12} \equiv -\frac{744}{12} \equiv -62 \equiv 707 \pmod{769},$$

and it can be easily verified from Jacobi's *Canon* that $13^{192} \equiv 707 \pmod{769}$.

Here, again, since $16r+1$, $16r+5$, $16r+9$, and $16r+13$ combine by multiplication in precisely the same way as 1, $-a/b$, -1, and $a/b \pmod p$, we can apply this process equally well if q be composite instead of prime; thus, since $293=17^2+2^2$, $17\equiv 2 \pmod{15}$, therefore -15, being of the form $16r+1$, is a quartic residue of 293.

4. If $\tan\theta' \equiv -1$; that is to say, if $a+b$ is divisible by q. Here, in a similar manner, we deduce

$$\left(\frac{q}{p}\right)_4 = 1,\ \frac{a}{b},\ -1,\ \text{or}\ -\frac{a}{b},$$

accordingly as q is of the form

$$16r+1,\quad 16r+5,\quad 16r+9,\quad 16r+13.$$

This might be at once inferred from the fact that a change of the sign of $\tan\theta$ is the result of writing $-a$ for a. Thus

$$\left(\frac{-35}{757}\right)_4 = -\frac{a}{b} = -\frac{9}{26},$$

since -35 is of the form $16r+13$, and $9+26 \equiv 0 \pmod{35}$.

$$\frac{-9}{26} \equiv \frac{-3\times 3}{26} \equiv \frac{754\times 3}{26} \equiv 29\times 3 \equiv 87 \pmod{757},$$

and we may verify from Jacobi's *Canon* that $(-35)^{189} \equiv 87 \pmod{757}$.

5. If $\tan\theta' \equiv 2$; that is to say, if $2a-b$ is divisible by q. Here the quartic residuacity of q, with respect to $a+bi$, is seen by Gauss' formula to be identical with that of q with respect to $1+2i$; consequently we deduce

$$\left(\frac{q}{p}\right)_4 = 1,\ -1,\ \frac{a}{b},\ \text{or}\ -\frac{a}{b},$$

accordingly as q is of the form

$$5r+1,\quad 5r+4,\quad 5r+3,\quad 5r+2;$$

that is to say, accordingly as q is of the form

$$20r+1,\ 20r+9,\ 20r+13,\ \text{or}\ 20r+17.$$

This again applies where q is composite.

[If q is of the form $20r+5$, the values $\tan\theta = 2$ can only occur where p is divisible by 5; that is to say, as p is supposed prime when $p=5$, so that in this case q is divisible by p.]

For example, to find $\left(\frac{-23}{641}\right)_4$, $641 = 25^2 + 4^2$ and

$$\tan\theta' \equiv \frac{4}{25} \equiv \frac{4}{2} \equiv 2 \pmod{23}.$$

Hence, -23 being of the form $20r+17$,

$$\left(\frac{-23}{641}\right)_4 = -\frac{a}{b} = -\frac{25}{4}.$$

We can verify from Jacobi's *Canon* that

$$(-23)^{160} \equiv 154 \equiv \frac{616}{4} \equiv \frac{-25}{4} \pmod{641}.$$

6. If $\tan\theta' \equiv -2$; that is to say, if $2a+b$ is divisible by q. Here, since a change in the sign of $\tan\theta$ is the result of writing $-a$ for a, we deduce that

$$\left(\frac{q}{p}\right)_4 = 1,\ -1,\ -\frac{a}{b},\ \text{or}\ \frac{a}{b},$$

accordingly as q is of the form

$$20r+1,\ 20r+9,\ 20r+13,\ \text{or}\ 20r+17.$$

7. If $\tan\theta' \equiv \frac{1}{2}$, that is to say if $a-2b$ is divisible by q, we have the trigonometrical relation

$$\tan^{-1}\tfrac{1}{2} = \tfrac{1}{2}\pi - \tan^{-1}2 = \tan^{-1}\infty + \tan^{-1}(-2).$$

Hence the quartic character indicated by $\tan\theta' \equiv \frac{1}{2}$ is the same as that indicated by $\tan\theta' \equiv -2$ if q is of the form $8r+1$ and the negative of that indicated by $\tan\theta' \equiv -2$ if q is of the form $8r+5$.

8. If $\tan\theta' \equiv -\frac{1}{2}$, we get in a similar manner that the quartic character indicated by $\tan\theta' \equiv -\frac{1}{2}$ is the same as that indicated by $\tan\theta' \equiv 2$ if q is of the form $8r+1$ and the negative of that indicated by $\tan\theta' \equiv 2$ if q is of the form $8r+5$.

So far the results are of a very special character, as it will only be in exceptional cases that $\tan\theta'$ will be congruent to one of the eight values $0, \infty, \pm 1, \pm 2, \pm\frac{1}{2}$. The argument in the case of 2, however, applies equally well to the case $\tan\theta' = r$, provided only $1+r^2$ is a prime number, so that we can find the quartic character indicated by any of the values $\pm 4, \pm 6, \pm 10, \pm 14, \pm 16, \pm 20, \pm 24, \pm 26$ and their reciprocals with the aid of Jacobi's *Canon*, as 17, 37, 101, 197, 257, 401, 577, and 677 are all primes occurring therein.

For instance in a case previously investigated by another method, we found $\left(\frac{67}{99889}\right)_4 = -1$. We might have proceeded thus

$$\tan\theta' \equiv \frac{230}{217} \equiv \frac{29}{16} \equiv \frac{96}{16} \equiv 6 \pmod{67},$$

but the quartic character indicated by 6 depends merely upon the residue (mod 37), and in particular

$$\left(\frac{-67}{37}\right)_4 = \left(\frac{7}{37}\right)_4 = \left(\frac{81}{37}\right)_4 = 1 \quad \text{(by inspection).}$$

Hence $$\left(\frac{-67}{99989}\right)_4 = 1 \ \text{and}\ \left(\frac{67}{99989}\right)_4 = -1.$$

Again, without the aid of the previous tables, we might find the value of $\left(\frac{-79}{8122369}\right)_4$. As before, we have $\tan\theta' = 14$, and the quartic character indicated by 14 depends merely on the residue of q (mod 197). But from Jacobi's *Canon*

$$\left(\frac{-79}{197}\right)_4 \equiv 183 \equiv -14 \equiv \frac{1}{14}.$$

Hence $$\left(\frac{-79}{8122369}\right) = \frac{a}{b} \text{ or } \frac{1537}{2400},$$

which agrees with the result previously obtained. The same method can be employed whenever $\tan\theta'$ can be reduced to the form $\pm k/l$ or $\pm l/k$, where l is supposed even and k^2+l^2 is a prime. If, for instance, we wish to find $\left(\frac{389}{40801}\right)_4$, we have from Cunningham's *Quadratic Partitions*

$$40801 = 201^2 + 20^2.$$

Therefore $$\tan\theta' \equiv \frac{20}{201} \equiv 33 \pmod{389}.$$

Now $33^2+1=1090$, a composite number, so that the methods so far considered are not available. With the help of Jacobi's or Cunningham's *Canon*, it is not difficult to find two small numbers having the ratio 33 (mod 389), and such that k^2+l^2 is a prime; thus, for instance, $33 \equiv \frac{396}{12} \equiv \frac{7}{12}$ (mod 389). By a generalization of the result given under 7 ($\tan\theta' \equiv \frac{1}{2}$), we know that the quartic character indicated by $\frac{7}{12}$ is the negative of that indicated by $\frac{-12}{7}$ (389 being of the form $8r+5$). But $\left(\frac{389}{193}\right)_4 = \left(\frac{3}{193}\right)_4 = 1$, so that the quartic character indicated by $\frac{7}{12}$ must be -1.

For the sake of clearness, we may put this last method in tabular form, dispensing with $\tan\theta'$ and giving the value of $(q/p)_4$ in terms of $(q/t)_4$: q is any number, positive or negative, prime or composite of the form $4n+1$; p is any prime of the form $4n+1$ and equal to a^2+b^2; t is any prime of the form $4n+1$ and equal to k^2+l^2.

No conventions are necessary as to the signs of a and b, but b and l are supposed even; the last convention, however, is not strictly necessary when q is of the form $8r+1$.

Table giving values of $(q/p)_4$ when $(q/t)_4$ is known.

	$q=8r+1$				$q=8r+5$			
Value of $(q/t)_4$	1	-1	k/l	$-k/l$	1	-1	k/l	$-k/l$
$b/a \equiv\ \ l/k \pmod q$	1	-1	a/b	$-a/b$	1	-1	a/b	$-a/b$
$b/a \equiv -l/k \pmod q$	1	-1	$-a/b$	a/b	1	-1	$-a/b$	a/b
$b/a \equiv\ \ k/l \pmod q$	1	-1	$-a/b$	a/b	-1	1	a/b	$-a/b$
$b/a \equiv -k/l \pmod q$	1	-1	a/b	$-a/b$	-1	1	$-a/b$	a/b

It need scarcely be remarked that if t is still too large for tables to be available, we may reduce q to its least residue $(\text{mod}\, t)$ and apply the process again, and so on indefinitely.

We now proceed to consider the case where $(1+r^2)$ or (k^2+l^2) is composite. For example, to start with the simplest instance:—

9. If $\tan\theta' = 3$; that is to say, if $3a-b$ is divisible by q. We have here the trigonometrical identity

$$\tan^{-1}3 = \tan^{-1}(-1) + \tan^{-1}(-2),$$

so that the quartic character indicated by 3 will be obtained by multiplying together those indicated by (-1) and (-2). The former depends on the residue of q (mod 16) and the latter on the residue of q (mod 20), so that, after 80, the values of q for which $(q/p)_4 = 1,\ -1,\ a/b$, or $-a/b$ will occur.

10. If $\tan\theta' = -3$, we may either merely alter the signs of a/b or $-a/b$, or use the identity

$$\tan^{-1}(-3) = \tan^{-1}1 + \tan^{-1}2.$$

11. If $\tan\theta' = \frac{1}{3}$, we have

$$\tan^{-1}\tfrac{1}{3} = \tan^{-1}2 + \tan^{-1}(-1).$$

12. If $\tan\theta' = -\frac{1}{3}$, we have

$$\tan^{-1}(-\tfrac{1}{3}) = \tan^{-1}1 + \tan^{-1}(-2).$$

A similar method can be applied when k^2+l^2 is any odd composite number, for, if e^2+f^2 be a prime factor of k^2+l^2, we have

$$\tan^{-1}\frac{k}{l}+\tan^{-1}\frac{e}{f}=\tan^{-1}\frac{kf+el}{lf-ek}$$

and
$$\tan^{-1}\frac{k}{l}-\tan^{-1}\frac{e}{f}=\tan^{-1}\frac{kf-el}{lf+ek},$$

and as is well known one or other of these two expression will have e^2+f^2 as a factor common to numerator and denominator, and when divided out will reduce to $\tan^{-1}g/h$, where $g^2+h^2=(k^2+l^2)/(e^2+f^2)$. The quartic character indicated by k/l is thus made to depend on that indicated by e/f and g/h. If g^2+h^2 is not prime, the process can be repeated until only prime factors are left. Thus, when finding $\left(\frac{389}{40801}\right)_4$ above, we might, after ascertaining $\tan\theta'\equiv 33 \pmod{389}$, have proceeded thus:

$$33^2+1=1090=10\times(3^2+10^2),$$

$$\tan^{-1}33+\tan^{-1}\frac{10}{3}=\tan^{-1}\left(-\frac{109}{327}\right)=\tan^{-1}\left(-\frac{1}{3}\right)=\tan^{-1}1+\tan^{-1}(-2),$$

so that $\quad \tan^{-1}33\equiv\tan^{-1}1+\tan^{-1}(-2)+\tan^{-1}\left(-\frac{10}{3}\right);$

389 is of form $16r+5$, so that 1 indicates quartic character a/b; 389 is of form $29r+9$, so that -2 indicates quartic character -1; 389 is of form $109r+62$ and

$$62^{27}\equiv 76\equiv -33\equiv -3\times 11\equiv\frac{-3}{10}\pmod{109};$$

and consequently $\left(-\frac{10}{3}\right)$ indicates quartic character a/b. Multiplying together, we have $(-a/b).(-1).a/b=-1$, so that $\left(\frac{389}{40801}\right)_4=-1$, which agrees with the result previously obtained.

If k and l are both odd numbers,

$$\tan^{-1}\frac{l}{k}=\tan^{-1}1+\tan^{-1}\frac{l-k}{l+k},$$

and as one of the numbers $(l-k)$ and $(l+k)$ is of the form $4r$ and the other of the form $4r+2$ this case is made to depend on the ordinary case, where one of the numbers k is odd and the other is even.

If $\tan\theta' = l/k$, we can at once determine the linear period of q after which the quadratic character indicated by l/k recurs.

If l is even, when l/k is reduced to its lowest terms, we have

$$\tan\frac{l}{k} = \tan^{-1}\frac{l_1}{k_1} + \tan^{-1}\frac{l_2}{k_2} + \tan^{-1}\frac{l_3}{k_3} + \ldots,$$

where $(k_1^2 + l_1^2)$, $(k_2^2 + l_2^3)$, $(k_3^2 + l_3^2)$, ... are the factors of which $k^2 + l^2$ is composed. Consequently the period of recurrence is the product of the prime factors multiplied by 4. If a factor is repeated several times, it must only be reckoned once in computing the period, for $n\tan^{-1} l_1/k_1$ only depends on $\tan^{-1} l_1/k_1$; and if n is a multiple of 4, the factor must be omitted altogether, for the quadratic character indicated by $4n\tan^{-1} l/k$ is always 1. Should $4n\tan^{-1} l_1/k_1$ be the only factor the period will be 4, as every number of the form $4r+1$ will then be a quadratic residue.

For instance, $5^4 = 625 = 7^2 + 24^2$. Consequently the quartic character indicated by $\dfrac{24}{7}$ is 1, and this result is independent of the value of q; thus if we had to find the values of $\left(\dfrac{3649}{94349}\right)_4$, we have, since

$$94349 = 307^2 + 10^2$$

and
$$\tan\theta' \equiv \frac{10}{307} \equiv \frac{24}{7} \pmod{3649},$$

$$\left(\frac{3649}{94349}\right)_4 = 1.$$

If l is odd and k is even the quartic character indicated by $\tan\theta'$ varies accordingly as q is of the form $8n+1$ or $8n+5$; consequently the recurring period is eight times the product of those prime factors of k^2+l^2 which do not occur an exact multiple of four times. Of course, if all prime factors occur exactly four times, the period is 8.

When both k and l are odd the quartic character indicated by $\tan\theta'$ varies according to whether q is of the form $16r+1$, $16r+5$, $16r+9$, or $16r+13$; and as 2 is one of the prime factors of (k^2+l^2), the recurring period is again eight times the product of those prime factors of k^2+l^2 which do not occur an exact multiple of four times.

The following table illustrates the recurring period for values of a/b and b/a not numerically greater than 8.

Table giving values of $(q/p)_4$.

(mod q)	Recurring Period	$(q/p)_4 = 1$	$(q/p)_4 = -1$	$(q/p)_4 = a/b$	$(q/p)_4 = -a/b$
$b \equiv 0$	$4r+$	1	—	—	—
$a \equiv 0$	$8r+$	1	5	—	—
$b/a \equiv 1$	$16r+$	1	9	13	5
$b/a \equiv -1$	$16r+$	1	9	5	13
$b/a \equiv 2$	$2\ r+$	1	9	13	17
$b/a \equiv -2$	$20r+$	1	9	17	13
$a/b \equiv 2$	$40r+$	1; 29	9; 21	13; 17	33; 37
$a/b \equiv -2$	$40r+$	1; 29	9; 21	33; 37	13; 17
$b/a \equiv 3$	$80r+$	1; 9; 53; 77	13; 37; 41; 49	17; 21; 29; 73	33; 57; 61; 69
$b/a \equiv -3$	$80r+$	1; 9; 53; 77	13; 37; 41; 49	33; 57; 61; 69	17; 21; 29; 73
$a/b \equiv 3$	$80r+$	1; 9; 13; 37	41; 49; 53; 77	21; 29; 33; 57	17; 61; 69; 73
$a/b \equiv -3$	$80r+$	1; 9; 13; 37	41; 49; 53; 77	17; 61; 69; 73	21; 29; 33; 57
$b/a \equiv 4$	$68r+$	1; 13; 21; 33	9; 25; 49; 53	5; 29; 37; 65	41; 45; 57; 61
$b/a \equiv -4$	$68r+$	1; 13; 21; 33	9; 25; 49; 53	41; 45; 57; 61	5; 29; 37; 65
$a/b \equiv 4$	$136r+$	1; 33; 53; 77 81; 89; 93; 117	9; 13; 21; 25 49; 69; 101; 121	5; 29; 37; 41 57; 113; 129; 133	45; 61; 65; 73 97; 105; 109; 125
$a/b \equiv -4$	$136r+$	1; 33; 53; 77 81; 89; 93; 117	9; 13; 21; 25 49; 69; 101; 121	45; 61; 65; 73 97; 105; 109; 125	5; 29; 37; 41 57; 113; 129; 133
$b/a \equiv 5$	$208r+$	1; 5; 25; 81 113; 121; 125; 141 149; 153; 189; 197	9; 17; 21; 37 45; 49; 85; 93 105; 109; 129; 185	29; 61; 69; 73 89; 97; 101; 137 145; 157; 161; 181	33; 41; 53; 57 77; 133; 165; 173 177; 193; 201; 205
$b/a \equiv -5$	$208r+$	1; 5; 25; 81 113; 121; 125; 141 149; 153; 189; 197	9; 17; 21; 37 45; 49; 85; 93 105; 109; 129; 185	33; 41; 53; 57 77; 133; 165; 173 177; 193; 201; 205	29; 61; 69; 73 89; 97; 101; 137 145; 157; 161; 181
$a/b \equiv 5$	$208r+$	1; 21; 25; 37 45; 81; 85; 93 109; 113; 121; 153	5; 9; 17; 49 105; 125; 129; 141 149; 185; 189; 197	29; 33; 41; 57 61; 69; 101; 157 177; 181; 193; 201	53; 73; 77; 89 97; 133; 137; 145 161; 165; 173; 205
$a/b \equiv -5$	$208r+$	1; 21; 25; 37 45; 81; 85; 93 109; 113; 121; 153	5; 9; 17; 49 105; 125; 129; 141 149; 185; 189; 197	53; 73; 77; 89 97; 133; 137; 145 161; 165; 173; 205	29; 33; 41; 57 61; 69; 101; 157 177; 181; 193; 201
$b/a \equiv 6$	$148r+$	1; 9; 33; 49; 53 81; 121; 137; 145	21; 25; 41; 65; 73 77; 85; 101; 141	29; 57; 61; 69; 89 105; 113; 125; 129	5; 13; 17; 45; 93 97; 109; 117; 133

Table giving values of $(q/p)_4$. *(cont.)*

(mod q)	Recurring Period	$(q/p)_4=1$	$(q/p)_4=-1$	$(q/p)_4=a/b$	$(q/p)_4=-a/b$
$b/a\equiv-6$	$148r+$	1; 9; 33; 49; 53 81; 121; 137; 145	21; 25; 41; 65; 73 77; 85; 101; 141	5; 13; 17; 45; 93 97; 109; 117; 133	29; 57; 61; 69; 89 105; 113; 125; 129
$a/b\equiv6$	$296r+$	1; 9; 21; 33; 49 77; 81; 85; 101; 121 137; 141; 145; 173 189; 201; 213; 221	25; 41; 53; 65; 73 149; 157; 169; 181; 197 225; 229; 233; 249 269; 285; 289; 293	17; 29; 61; 69; 97 125; 153; 161; 193; 205 237; 241; 253; 257 261; 265; 277; 281	5; 13; 45; 57; 89 93; 105; 109; 113; 117 129; 133; 165; 177 209; 217; 245; 273
$a/b\equiv-6$	$296r+$	1; 9; 21; 33; 49 77; 81; 85; 101; 121 137; 141; 145; 173 189; 201; 213; 211	25; 41; 53; 65; 73 149; 157; 169; 181; 197 225; 229; 233; 249 269; 285; 289; 293	5; 13; 45; 57; 89 93; 105; 109; 113; 117 129; 133; 165; 177 209; 217; 245; 273	17; 29; 61; 69; 97 125; 153; 161; 193; 205 237; 241; 253; 257 261; 265; 277; 281
$b/a\equiv7$	$80r+$	1; 49; 57; 73	9; 17; 33; 41	13; 21; 69; 77	29; 37; 53; 61
$b/a\equiv-7$	$80r+$	1; 49; 57; 73	9; 17; 33; 41	29; 37; 53; 61	13; 21; 69; 77
$a/b\equiv7$	$80r+$	1; 49; 57; 73	9; 17; 33; 41	13; 21; 69; 77	29; 37; 53; 61
$a/b\equiv-7$	$80r+$	1; 49; 57; 73	9; 17; 33; 41	29; 37; 53; 61	13; 21; 69; 77
$b/a\equiv8$	$260r+$	1; 33; 49; 57 61; 69; 73; 81 97; 129; 193; 197	9; 29; 37; 93 101; 121; 137; 177 181; 209; 213; 253	21; 109; 141; 149 153; 157; 173; 217 233; 237; 241; 249	17; 41; 53; 77 89; 113; 133; 161 189; 201; 229; 257
$b/a\equiv-8$	$260r+$	1; 33; 49; 57 61; 69; 73; 81 97; 129; 193; 197	9; 29; 37; 93 101; 121; 137; 177 181; 209; 213; 253	17; 41; 53; 77 89; 113; 133; 161 189; 201; 229; 257	21; 109; 141; 149 153; 157; 173; 217 233; 237; 241; 249
$a/b\equiv8$	$52\ r+$	1; 29; 33; 37 49; 57; 73; 81 93; 97; 101; 129 181; 193; 213; 253 269; 321; 329; 381 397; 437; 457; 469	9; 61; 69; 121 137; 177; 197; 209 261; 289; 293; 297 309; 317; 333; 341 353; 357; 361; 389 441; 453; 473; 513	17; 21; 41; 89 109; 113; 141; 149 157; 161; 173; 201 237; 257; 313; 337 393; 413; 449; 477 489; 493; 501; 509	53; 77; 133; 153 189; 217; 229; 233 241; 249; 277; 281 301; 349; 369; 373 401; 409; 417; 421 433; 461; 497; 517
$a/b\equiv-8$	$520r+$	1; 29; 33; 37 49; 57; 73; 81 93; 97; 101; 129 181; 193; 213; 253 269; 321; 329; 381 397; 437; 457; 469	9; 61; 69; 121 137; 177; 197; 209 261; 289; 293; 297 309; 317; 333; 341 353; 357; 361; 389 441; 453; 473; 513	53; 77; 133; 153 189; 217; 229; 233 241; 249; 277; 281 301; 349; 369; 373 401; 409; 417; 421 433; 461; 497; 517	17; 21; 41; 89 109; 113; 141; 149 157; 161; 173; 201 237; 257; 313; 337 393; 413; 449; 477 489; 493; 501; 509

The quantities in the body of the table are the different values of q. There is no restriction on the value of q beyond the fact that it is supposed to be of the form $4n+1$, and it may accordingly be prime or composite, positive or negative; and the table can be used to find the quartic residuacity of q, no matter how large q may be, provided only the value of b/a or a/b falls within the tables. To show how the table may be used to find the quartic residuacity, we may take $\left(\dfrac{271}{58997}\right)_4$, $58997 = 89^2 + 226^2$:

$$\frac{b}{a} = \frac{226}{89} \equiv \frac{-45}{89} \equiv \frac{135}{-267} \equiv \frac{-136}{4} \equiv -34 \pmod{271},$$

-34 is not within the limit of the table, but its reciprocal -8 happens to be so. Thus $a/b \equiv -8 \pmod{271}$.

Since -271 is of the form $520r + 249$, we have

$$\left(\frac{-271}{58997}\right)_4 = \frac{a}{b},$$

as 249 occurs in the third column of the table; and, since 58927 is of the form $8r+5$,

$$\left(\frac{271}{58997}\right)_4 = -\left(\frac{-271}{58997}\right)_4 = -\frac{a}{b}.$$

If our table had only extended as far as 5, we could still have reduced the question to within the limits of the table, for

$$\tan^{-1}(-\tfrac{1}{8}) = \tan^{-1}3 + \tan^{-1}(-5),$$

$-271 = 80r + 49$, and 49 occurs in the second column,

when $b/a \equiv 3$,

$-271 = 208r + 145$, and 145 occurs in the fourth column,

when $b/a \equiv -5$,

so that $\left(\dfrac{-271}{58997}\right)_4 = (-1) \times \left(-\dfrac{a}{b}\right) = \dfrac{a}{b}$, as before

We can easily deduce the law of quartic reciprocity for two imaginary numbers. Thus let $p = a^2 + b^2$ and $t = k^2 + l^2$, where p and t are primes of the form $4r+1$. Then we have to find the relation between $\left(\dfrac{k+li}{a+bi}\right)_4$ and $\left(\dfrac{a+bi}{k+li}\right)_4$. We shall suppose b and l even and k and a both of the form $(4r+1)$.

If either $k+li$ or $a+bi$ are not of this form, they can be reduced to it by multiplication by some power of i; and as the value of $\left(\dfrac{i}{a+bi}\right)_4 = i^{\frac{1}{4}(p-1)}$ is easily found, this assumption involves no loss of generality.

Let $q = ak + bl$, then q is of the form $4r+1$; and applying the relation between $\left(\dfrac{q}{p}\right)_4$ and $\left(\dfrac{q}{t}\right)_4$ previously found, we have, since $\dfrac{b}{a} \equiv -\dfrac{k}{l} \pmod{q}$, when q is of the form $8r+1$,

$$\left(\frac{q}{p}\right)_4 = 1,\ -1,\ \frac{a}{b},\ \text{or}\ -\frac{a}{b},$$

accordingly as $\left(\dfrac{q}{t}\right)_4 = 1,\ -1,\ \dfrac{k}{l},\ \text{or}\ -\dfrac{k}{l}.$

But $\dfrac{a}{b} = -i \pmod{a+bi}$ and $\dfrac{k}{l} = -i \pmod{k+li}$. Therefore, when q is of the form $8r+1$,

$$\left(\frac{q}{a+bi}\right)_4 = \left(\frac{q}{k+li}\right)_4.$$

Similarly, when q is of the form $8r+5$,

$$\left(\frac{q}{a+bi}\right)_4 = -\left(\frac{q}{k+li}\right)_4.$$

Hence

$$\left(\frac{q}{a+bi}\right)_4 \left(\frac{q}{k+li}\right)_4 = (-1)^{\frac{1}{4}(q-1)} = (-1)^{\frac{1}{4}(a-1)}.(-1)^{\frac{1}{4}(k-1)}.(-1)^{\frac{1}{4}bl}.$$

for $\quad q-1 = \{(a-1)+1\}\{(k-1)+1\} + bl - 1$

$$= (a-1)(k-1) + (a-1) + (k-1) + bl,$$

and $(a-1)(k-1)$ is a multiple of 16. But

$$q = ak + bl \equiv a(k+li) \pmod{a+bi},$$

and we know that (since a is a factor of a) $\left(\frac{a}{p}\right)_4$ and consequently $\left(\frac{a}{a+bi}\right)_4 = (-1)^{\frac{1}{4}(a-1)}$; therefore

$$\left(\frac{q}{a+bi}\right)_4 = (-1)^{\frac{1}{4}(a-1)}\left(\frac{k+li}{a+bi}\right)_4.$$

Similarly $$\left(\frac{q}{k+li}\right)_4 = (-1)^{\frac{1}{4}(k-1)}\left(\frac{a+bi}{k+li}\right)_4;$$

therefore $$\left(\frac{k+li}{a+bi}\right)_4 = \left(\frac{a+bi}{k+li}\right)_4 \times (-1)^{\frac{1}{4}bl}.$$

Having established the law for the case where a and k are both of the form $4r+1$, it is easy to extend it to the case where either or both are of the form $4r-1$ by simply applying the law to $-(k+li)$ or $-(a+bi)$, as the case may be, and restoring the original signs by introducing factors $\left(\frac{-1}{a+bi}\right)_4$ or $\left(\frac{-1}{k+li}\right)_4$. The result is

$$\left(\frac{k+li}{a+bi}\right)_4 = \left(\frac{a+bi}{k+li}\right)_4 \times (-1)^{\frac{1}{4}\{bl+l(a-1)+b(k-1)\}},$$

this is accordingly true whether a and k are of the form $4r+1$ or $4r-1$.

$(k+li)^{\frac{1}{4}(p-1)}$ (mod p) may have any one of the following 16 values:

$$\pm 1,\ \pm i,\ \pm\frac{a}{b},\ \pm\frac{a}{b}i,\ \pm\frac{a\pm b}{2b}(1\pm i).$$

If we write $\left(\frac{k+li}{p}\right)_4$ for the particular one of these 16 values to which $(k+li)^{\frac{1}{4}(p-1)}$ is congruent, we may find the relation that subsists between $\left(\frac{k+li}{p}\right)_4$ and $\left(\frac{a+bi}{t}\right)_4$. The value of $\left(\frac{k+li}{p}\right)_4$ can of course be determined from the values of $\left(\frac{k+li}{a+bi}\right)_4$ and $\left(\frac{k+li}{a+bi}\right)_4$, and similarly with $\left(\frac{a+bi}{t}\right)_4$. We accordingly tabulate the relation between $\left(\frac{k\pm li}{p}\right)_4$ and $\left(\frac{a\pm bi}{t}\right)_4$.

$\left(\frac{k+li}{p}\right)_4$	$\left(\frac{k-li}{p}\right)_4$	$\left(\frac{t}{p}\right)_4$	$\left(\frac{a+bi}{t}\right)_4 \times (-1)^{\frac{1}{4}bl}$	$\left(\frac{a-bi}{t}\right)_4 \times (-1)^{\frac{1}{4}bl}$	$\left\{\frac{(a+bi)/(a-bi)}{t}\right\}_4$
± 1	± 1	1	± 1	± 1	1
$\pm i$	$\mp i$	1	$\mp \frac{k}{l}$	$\mp \frac{k}{l}$	1
$\pm \frac{a}{b}$	$\pm \frac{a}{b}$	-1	$\mp i$	$\pm i$	-1
$\pm \frac{a}{b} i$	$\mp \frac{a}{b} i$	-1	$\pm \frac{k}{l} i$	$\mp \frac{k}{l} i$	-1
$\pm \frac{a+b}{2b}(1+i)$	$\pm \frac{a+b}{2b}(1-i)$	$\frac{a}{b}$	$\mp \frac{k-l}{2l}(1-i)$	$\mp \frac{k-l}{2l}(1+i)$	$-i$
$\pm \frac{a+b}{2b}(1-i)$	$\pm \frac{a+b}{2b}(1+i)$	$\frac{a}{b}$	$\pm \frac{k+l}{2l}(1-i)$	$\pm \frac{k+l}{2l}(1+i)$	$-i$
$\pm \frac{a-b}{2b}(1+i)$	$\pm \frac{a-b}{2b}(1-i)$	$-\frac{a}{b}$	$\pm \frac{k-l}{2l}(1+i)$	$\pm \frac{k-l}{2l}(1-i)$	i
$\pm \frac{a-b}{2b}(1-i)$	$\pm \frac{a-b}{2b}(1+i)$	$-\frac{a}{b}$	$\mp \frac{k+l}{2l}(1+i)$	$\mp \frac{k+l}{2l}(1-i)$	i

We see from this table that the value of $\left(\frac{k+li}{p}\right)_4$ uniquely determines the value of $\left(\frac{a+bi}{t}\right)_4$, and *vice versâ*. The table also shows how the use of $\frac{a+bi}{a-bi}$ in Gauss' form of the law applicable to real primes eliminates the coefficients $\frac{k}{l}$ and $\frac{k \pm l}{2l}$ and also gets rid of the coefficient $(-1)^{\frac{1}{4}\{bl+l(a-1)+l(k-1)\}}$ [written $(-1)^{\frac{1}{4}bl}$ in table], so that all conventions as to the sign of a and k become unnecessary.

When p is a prime of the form $4r-1$, $\left(\frac{k+li}{p}\right)_4$ means the residue ± 1, $\pm i$ of $(k+li)^{\frac{1}{4}(p^2-1)} \pmod p$. We can find this residue as follows. By the Binomial Theorem

$$(k+li)^p \equiv k^p + (li)^p \equiv k - li \pmod p,$$

for all the intermediate terms contain p as a factor. Therefore

$$(k+li)^{p-1} \equiv \frac{k-li}{k+li} \pmod p$$

and
$$(k+li)^{\frac{1}{4}(p^2-1)} \equiv \left(\frac{k-li}{k+li}\right)^{\frac{1}{4}(p+1)} \pmod p.$$

But by the ordinary form of Gauss' law the last expression gives the value of $\left(\frac{-p}{k+li}\right)_4$. So that we have

$$\left(\frac{k+li}{p}\right)_4 = \left(\frac{-p}{k+li}\right)_4$$

independently of any convention as to the sign of k. So that the law of reciprocity

$$\left(\frac{k+li}{a+bi}\right)_4 = \left(\frac{a+bi}{k+li}\right)_4 \times (-1)^{\frac{1}{4}\{bl+l(a-1)+b(k-1)\}}$$

continues to hold true for the case when $b=0$; for a in that case to be a prime in the complex system must be of the form $4r-1$, and the final coefficient reduces to $(-1)^{\frac{1}{4}l}$, which expresses the value of $\left(\frac{-1}{k+li}\right)_4$. If a is taken negatively, it is easy to verify that the formula still remains true. If l and b are both zero, the formula reduces to $\left(\frac{k}{a}\right)_4 = \left(\frac{a}{k}\right)_4$. This is obviously true, for in the complex system every real number is a $(p+1)^{\text{ic}}$ residue of any prime p of the form $4r-1$, and $p+1$ is a multiple of 4.

EXPRESSIONS FOR THE VOLUME OF A TETRAHEDRON.

By *Professor Anglin*, University College, Cork.

It is proposed to obtain expressions for the volume of a tetrahedron involving the coordinates of its vertices by a method which, I believe, has not hitherto been employed, and which applies alike to rectangular and oblique axes.

1. We first take the case of a tetrahedron having one vertex at the origin O, and whose base is the triangle PQR, the coordinates of whose vertices are given.

If the plane of PQR meet the coordinate axes in A, B, C respectively, since the tetrahedra $OPQR$ and $OABC$ have the same altitude, their volumes are as the areas of their bases PQR and ABC, which are as the areas of their projections on the plane of yz; that is, as

$$\begin{vmatrix} y_1, & z_1, & 1 \\ y_2, & z_2, & 1 \\ y_3, & z_3, & 1 \end{vmatrix} \text{ is to } OB.OC,$$

which holds alike for rectangular and oblique axes. But six times the volume of the tetrahedron

$$OABC = OA.OB.OC.2n,$$

where, with the usual notation,

$$4n^2 = 1 - \cos^2\alpha - \cos^2\beta - \cos^2\gamma + 2\cos\alpha\cos\beta\cos\gamma,$$

α, β, γ being the angles between the coordinate axes. Thus we have

$$6 \text{ vol. } OPQR = \begin{vmatrix} y_1, & z_1, & 1 \\ y_2, & z_2, & 1 \\ y_3, & z_3, & 1 \end{vmatrix} \times OA.2n.$$

But, writing down the equation to the plane through P, Q, R, and putting $y=0$, $z=0$, we get

$$\begin{vmatrix} y_1, & z_1, & 1 \\ y_2, & z_2, & 1 \\ y_3, & z_3, & 1 \end{vmatrix} OA = \begin{vmatrix} x_1, & y_1, & z_1 \\ x_2, & y_2, & z_2 \\ x_3, & y_3, & z_3 \end{vmatrix}.$$

Hence $\qquad 6 \text{ vol. } OPQR = (x_1, y_2, z_3)\, 2n.$

Now taking any tetrahedron $PQRS$, since from the geometry of the figure it is equal to the algebraic sum of the four tetrahedra with common vertex O and bases the faces of $PQRS$, we have

$$6 \text{ vol. } PQRS = \{(x_2y_3z_4) - (x_1y_3z_4) + (x_1y_2z_4) - (x_1y_2z_3)\}\, 2n$$

$$= \begin{vmatrix} x_1, & y_1, & z_1, & 1 \\ x_2, & y_2, & z_2, & 1 \\ x_3, & y_3, & z_3, & 1 \\ x_4, & y_4, & z_4, & 1 \end{vmatrix} 2n.$$

The volume of a tetrahedron, when the equations to the faces are given in the form $ax+by+cz+d=0$, may be readily deduced by finding the coordinates of the vertices, which are given by equations of the form

$$\frac{x}{(b_1c_2d_3)} = \frac{-y}{(a_1c_2d_3)} = \frac{z}{(a_1b_2d_3)} = \frac{-1}{(a_1b_2c_3)},$$

and substituting in the above expression, when we shall get

$$6 \text{ vol. } = 2n\,(a_1b_2c_3d_4)^3/P,$$

where P is the product of the minors of the determinant $(a_1b_2c_3d_4)$ with respect to the elements of the last column.

2. Expressions for the volume of a tetrahedron involving the quadriplanar and tetrahedral coordinates of its vertices may now be obtained. We shall exhibit the work in the latter system, as it is somewhat simpler than in the former.

If $ABCD$ be the tetrahedron of reference, we take one vertex D as origin and transform to oblique Cartesians with DA, DB, DC as axes. Thus, if x, y, z, u be the tetrahedral and x', y', z' the Cartesian coordinates of any point P, since x is equal to the ratio of the perpendiculars on the face BCD from P and A, we have

$$x = x'/DA, \quad y = y'/DB, \quad z = z'/DC.$$

Hence, if the edges DA, DB, DC be equal to a, b, c respectively, substituting in the expression for the volume in Cartesians, we get

$$6 \text{ vol. } PQRS = \begin{vmatrix} ax_1, & by_1, & cz_1, & x_1+y_1+z_1+u_1 \\ \vdots & \vdots & \vdots & \vdots \end{vmatrix} 2n$$

$$= \begin{vmatrix} x_1, & y_1, & z_1, & u_1 \\ x_2, & y_2, & z_2, & u_2 \\ x_3, & y_3, & z_3, & u_3 \\ x_4, & y_4, & z_4, & u_4 \end{vmatrix} 2nabc;$$

that is, $\qquad \text{vol. } PQRS = (x_1,\ y_2,\ z_3,\ u_4)\, V,$

where V is the volume of the tetrahedron of reference.

The vo.ume in quadriplanars may be obtained in like manner from that in Cartesians; but it may also be deduced at once from that in tetrahedrals by the substitutions

$$3V = A\alpha/x = B\beta/y = C\gamma/z = D\delta/u,$$

where A, B, C, D are the areas of the faces of the tetrahedron of reference, when we shall get

$$\text{vol. } PQRS = (\alpha_1\beta_2\gamma_3\delta_4)\frac{ABCD}{3^4 V^3}.$$

If the equations to the faces of the tetrahedron be given in the form $l\alpha + m\beta + n\gamma + r\delta = 0$ in quadriplanars, we may find the coordinates of the vertices, which are given by equations of the form

$$\frac{\alpha}{(m_1n_2r_3)} = \frac{-\beta}{(l_1n_2r_3)} = \frac{\gamma}{(l_1m_2r_3)} = \frac{-\delta}{(l_1m_2n_3)} = \frac{3V}{(123)},$$

where (123) denotes

$$\begin{vmatrix} A, & B, & C, & D \\ l_1, & m_1, & n_1, & r_1 \\ l_2, & m_2, & n_2, & r_2 \\ l_3, & m_3, & n_3, & r_3 \end{vmatrix};$$

and substituting in the above expression, we shall get

$$\frac{ABCD\,(l_1m_2n_3r_4)^3.\,V}{(234)\,(134)\,(124)\,(123)}$$

for the volume in quadriplanars; and the expression for the volume in tetrahedrals is what this becomes by replacing each of the letters A, B, C, D by unity.

NOTES ON INTEGRAL EQUATIONS.

By *H. Bateman.*

VII.

The solution of partial differential equations by means of definite integrals.

1. It is well known that the partial differential equation

$$\frac{\partial^2 V}{\partial x^2} + \frac{\partial^2 V}{\partial y^2} + k^2 V = 0 \text{.....................} (1)$$

possesses the particular solution

$$V = J_0[k\sqrt{\{(x-a)^2+y^2\}}],$$

and that this solution may be generalised by forming the definite integral

$$V = \int_{-\infty}^{\infty} J_0[k\sqrt{\{(x-a)^2+y^2\}}] f(a)\, da \text{.......} (2).$$

The characteristic properties of a solution which is capable of being represented in this form have not been fully discussed, nor has the question of the uniqueness of the representation been answered. I have thought it worth while then to study a few definite integrals of this type in the hope of obtaining a partial answer to the questions at issue. The results which are obtained may be regarded as typical for a large class of definite integral solutions of partial differential equations.

2. The first problem is to obtain representations of the particular solutions

$$\cos \mu x . \cos y\sqrt{(k^2-\mu^2)}, \quad \sin \mu x . \cos y\sqrt{(k^2-\mu^2)}$$

in the form (2). This may be solved with the aid of Fourier's formula as follows: It is known that

$$\int_0^{\frac{1}{2}\pi} \cos(\xi \sin\theta) \cos(\eta\cos\theta)\, d\theta = \tfrac{1}{2}\pi J_0\{\sqrt{(\xi^2+\eta^2)}\}.$$

Put $\xi = kx$, $\eta = ky$, $\mu = k\sin\theta$, then this formula gives

$$\int_0^k \cos(\mu x)\,.\cos y\sqrt{(k^2-\mu^2)}\,\frac{d\mu}{\sqrt{(k^2-\mu^2)}} = \tfrac{1}{2}\pi J_0\{k\sqrt{(x^2+y^2)}\}.$$

Hence it follows that

$$\int_0^k \cos\mu a\,.\cos\mu x\,.\cos y\sqrt{(k^2-\mu^2)}\,\frac{2d\mu}{\sqrt{(k^2-\mu^2)}}$$

$$= \tfrac{1}{2}\pi\left[J_0\{k\sqrt{((x-a)^2+y^2)}\} + J_0\{k\sqrt{((x+a)^2+y^2)}\}\right].$$

Inverting this equation by means of Fourier's formula

$$\int_0^k \cos\mu a\,.\,\phi(\mu)\,d\mu = f(a),$$

$$\begin{aligned}\int_0^\infty \cos\mu a\,.\,f(a)\,da &= \phi(\mu) \qquad (\mu < k)\\ &= 0 \qquad\quad\; (\mu > k),\end{aligned}$$

we find that

$$\int_0^\infty \cos\mu a\left[J_0\{k\sqrt{((x-a)^2+y^2)}\} + J_0\{k\sqrt{((x+a)^2+y^2)}\}\right]da$$

$$\begin{aligned}&= \frac{2}{\sqrt{(k^2-\mu^2)}}\cos\mu x\,.\cos y\sqrt{(k^2-\mu^2)} \qquad (\mu^2 < k^2)\\ &= 0 \qquad (\mu^2 > k^2).\end{aligned}$$

Changing a into $-a$ in the second half of the integral, we obtain the required representation:

$$\int_{-\infty}^\infty J_0[k\sqrt{\{(x-a)^2+y^2\}}]\cos\mu a\,.\,da$$

$$\begin{aligned}&= \frac{2}{\sqrt{(k^2-\mu^2)}}\cos\mu x\,.\cos y\sqrt{(k^2-\mu^2)} \qquad (\mu^2 < k^2)\\ &= 0 \qquad (\mu^2 > k^2) \qquad\qquad (3).\end{aligned}$$

The function $\phi(\mu) = \dfrac{2\cos\mu x\,.\cos y\sqrt{(k^2-\mu^2)}}{\sqrt{(k^2-\mu^2)}}$ becomes infinite when $\mu = k$; but we can easily convince ourselves that Fourier's formula is applicable by applying the formula to the difference

$$\frac{2\cos\mu x\,.\cos y\sqrt{(k^2-\mu^2)}}{\sqrt{(k^2-\mu^2)}} - \frac{2\cos\mu x}{\sqrt{(k^2-\mu^2)}},$$

which is finite when $\mu = k$ and satisfies Dirichlet's conditions.

The formula obtained by putting $y=0$ is certainly valid, for the equation

$$\int_{-\infty}^{\infty} J_0\{k(x-a)\}\cos\mu a\,.\,da = \frac{2}{\sqrt{(k^2-\mu^2)}}\cos\mu x \quad (\mu^2<k^2)$$
$$= 0 \quad (\mu^2>k^2)$$

may be deduced at once from Weber's formula*

$$\tfrac{1}{2}\int_{-\infty}^{\infty} J_0(kz)\cos\mu z\,dz = \frac{1}{\sqrt{(k^2-\mu^2)}} \quad (\mu^2<k^2)$$
$$= 0 \quad (\mu^2>k^2)$$

by putting $x-a=z$. In a similar way it can be shown that

$$\int_{-\infty}^{\infty} J_0[k\sqrt{\{(x-a)^2+y^2\}}]\sin\mu a\,.\,da$$
$$= \frac{2}{\sqrt{(k^2-\mu^2)}}\sin\mu x\,.\cos y\sqrt{(k^2-\mu^2)} \quad (\mu^2<k^2)$$
$$= 0 \quad (\mu^2>k^2) \qquad\qquad (4).$$

Thus the particular solutions

$$\cos\mu x\,.\cos y\sqrt{(k^2-\mu^2)}, \quad \sin\mu x\,.\cos y\sqrt{(k^2-\mu^2)}$$

may be expressed in the form (2); but I do not see how to obtain corresponding expressions for the particular solutions $\cos\mu x\,.\sin y\sqrt{(k^2-\mu^2)}$ and $\sin\mu x\,.\sin y\sqrt{(k^2-\mu^2)}$.

3. Equation (3) may be written in another form by putting

$$\mu = m\sin\theta = k\sin\phi,$$

where $m>k$. Thus

$$\tfrac{1}{2}m\cos\theta\int_{-\infty}^{\infty} J_0[k\sqrt{\{(x-a)^2+y^2\}}]\cos(ma\sin\theta)\,da$$
$$= \cos(kx\sin\phi)\cos(ky\cos\phi)\frac{m\cos\theta}{k\cos\phi} \quad (\phi<\tfrac{1}{2}\pi)$$
$$= 0 \quad \left(\sin\theta<\frac{k}{m}\right).$$

* *Crelle's Journal*, bd. 75 (1873).

Multiply this equation by $F(m\sin\theta)\,d\theta$ and integrate with regard to θ between 0 and $\frac{1}{2}\pi$; then, since

$$F(m\sin\theta)=F(k\sin\phi),\qquad m\cos\theta\,.\,d\theta=k\cos\phi\,.\,d\phi,$$

we obtain the relation

$$\tfrac{1}{2}\int_{-\infty}^{\infty} J_0[k\sqrt{\{(x-a)^2+y^2\}}]\,G(m,a)\frac{da}{a}$$
$$=\int_0^{\frac{1}{2}\pi}\cos(kx\sin\phi)\cos(ky\cos\phi)\,F(k\sin\phi)\,d\phi\ \ldots.(5),$$

where $\quad G(m,a)=ma\int_0^{\frac{1}{2}\pi}\cos(ma\sin\theta)\,F(m\sin\theta\cos\theta\,d\theta.$

The change in the order of integration in the repeated integral is not easy to justify by the ordinary rules, because the integral

$$\int_{-\infty}^{\infty} J_0[k\sqrt{\{(x-a)^2+y^2\}}]\cos(ma\sin\theta)\,da$$

is discontinuous. It is easy to see, however, that the integral

$$\int_{-\infty}^{\infty}[J_0\{k\sqrt{((x-a)^2+y^2)}\}-J_0\{k(x-a)\}]\cos(ma\sin\theta)\,da$$

is uniformly convergent in the interval $0<\theta<\frac{1}{2}\pi$, for the integral

$$\int_{-\infty}^{\infty}|\,J_0[k\sqrt{\{(x-a)^2+y^2\}}]-J_0\{k(x-a)\}\,|\,da$$

is convergent. The change in the order of integration is therefore justifiable when $F(m\sin\theta)$ is finite, provided it is justifiable in the case when $y=0$. When $y=0$ equation (5) may be written

$$\tfrac{1}{2}\int_0^{\infty}[J_0\{k(x-a)\}+J_0\{k(x+a)\}]\,da\int_0^m\cos(az)\,F(z)\,dz$$
$$=\int_0^{\frac{1}{2}\pi}\cos(kx\sin\phi)\,F(k\sin\phi)\,d\phi\ldots\ldots.(6)$$

or

$$\int_0^{\infty}da\left\{\int_0^{\frac{1}{2}\pi}\cos(kx\sin\phi)\cos(ka\sin\phi)\,d\phi\right\}\int_0^m\cos az\,F(z)\,dz$$
$$=\int_0^{\frac{1}{2}\pi}\cos(kx\sin\phi)\,F(k\sin\phi)\,d\phi\ldots\ldots(7).$$

Now the integral

$$\int_0^\infty \cos(ka\sin\phi)\int_0^m \cos az\, F(z)\, dz$$

is uniformly convergent* for $k<m$, and is equal to $F(k\sin\phi)$; hence the order of integration may be changed in (7), and the equation becomes an identity.

Equation (5) indicates that the function

$$V=\int_0^{\frac{1}{2}\pi}\cos(kx\sin\phi)\cos(ky\cos\phi)\,F(k\sin\phi)\,d\phi\;\ldots(8),$$

which is a particular solution of (1), can be expressed in the form (2) in a variety of ways. We have, in fact,

$$V=\tfrac{1}{2}\int_{-\infty}^\infty J_0[k\surd\{(x-a)^2+y^2\}]\,G(m,a)\frac{da}{a}\;\ldots\ldots(9),$$

where m has any value greater than or equal to k. In the particular case when $F=1$, this equation becomes

$$J_0\{k\surd(x^2+y^2)\}=\frac{1}{\pi}\int_{-\infty}^\infty J_0[k\surd\{(x-a)^2+y^2\}]\sin ma\frac{da}{a}\ldots(10)$$

or

$$J_0\{k\surd(x^2+y^2)\}=\frac{1}{\pi}\int_{-\infty}^\infty \frac{\sin m(x-z)}{x-z}J_0\{k\surd(z^2+y^2)\}\,dz.$$

This verifies Hardy's result† that $J_0\{k\surd(x^2+y^2)\}$ is an m-function for $m\geq k$.

It follows from equation (9) that the solution of the integral equation

$$f(x)=\int_{-\infty}^\infty J_0[k\surd\{(x-a)^2+y^2\}]\,\phi(a)\,da$$

is not unique, for the homogeneous equation

$$0=\int_{-\infty}^\infty J_0[k\surd\{(x-a)^2+y^2\}]\,\chi(a)\,da$$

possesses innumerable solutions of the type

$$\chi(a)=\frac{1}{a}\{G(m,a)-G(n,a)\}\qquad(m>n\geq k),$$

where $G(m,a)=ma\int_0^{\frac{1}{2}\pi}\cos(ma\sin\theta)\,F(m\sin\theta)\cos\theta\,d\theta.$

* See the footnote to p. 100. It will be assumed that $F(z)$ is continuous and of limited total fluctuation.

† *Proc. Lond. Math. Soc*, vol. vii., p. 464.

Another interesting consequence of equation (9) is derived by putting $a = x - z$. It appears that for certain types of function $f(x)$ the solution of the integral equation

$$f(x) = \int_{-\infty}^{\infty} \frac{G(m, x-z)}{x-z} \psi(z) \ldots\ldots\ldots\ldots (11)$$

is the same for all values of m greater than a certain number k. This is a generalisation of the result obtained by Hardy for the case of the equation

$$f(x) = \int_{-\infty}^{\infty} \frac{\sin m(x-z)}{x-z} \psi(z)\, dz.$$

4. The artifice which was used to justify the change in the order of integration in a repeated integral is really of wide application. In its simplest form the artifice is as follows.

Let
$$\int_0^k \cos(xz)\, \phi(z)\, dz = f(x) \ldots\ldots\ldots\ldots\ldots\ldots (12)$$

be an integral equation which can be inverted by means of Fourier's formula

$$\begin{aligned} \int_0^{\infty} \cos(xz) f(x)\, dx &= \phi(z) \quad (z < k) \\ &= 0 \quad\quad (z > k). \end{aligned}$$

The integral on the left-hand side is sometimes non-uniformly convergent in the vicinity of $z = k$, consequently, if $m > k$, there is some doubt as to whether we can change the order of integration in the repeated integral

$$\int_0^m g(z)\, dz \int_0^{\infty} \cos(xz) f(x)\, dx$$

and write

$$\int_0^{\infty} f(x)\, dx \int_0^m \cos(xz)\, g(z)\, dz = \int_0^k \phi(z)\, g(z)\, dz \ldots (13).$$

The change in the order of integration is certainly justifiable if this last equation is true. Now, if we replace $f(x)$ by the definite integral (12), the repeated integral on the left-hand side of (13) becomes

$$\int_0^{\infty} dx \int_0^k \cos(xu)\, \phi(u)\, du \int_0^m \cos(xz)\, g(z)\, dz,$$

and it is allowable to change the order of integration with regard to x and u, for the integral

$$\int_0^\infty \cos(xu)\,dx \int_0^m \cos(xz)\,g(z)\,dz = g(u)$$

is uniformly convergent* for $(0 \leq u \leq k)$, if $g(z)$ is continuous, and of limited total fluctuation in the interval $(0 < z < m)$.

Changing the order of integration, and substituting the value of the last integral, we obtain

$$\int_0^k \phi(u)\,g(u)\,du,$$

which is equal to the right-hand side of (13). A similar artifice may be used for discontinuous integrals depending on $\sin(xz)$ instead of $\cos(xz)$; for instance, if we take the discontinuous integral†

$$\begin{aligned} \int_0^\infty \sin xt\,.\,J_0(zt)\,dt &= \frac{1}{\sqrt{(x^2-z^2)}} \qquad (x > z) \\ &= 0 \qquad\qquad\qquad (x < z), \end{aligned}$$

it is legitimate to change the order of integration when we multiply by $\cos^{-1} x\,dx$ and integrate between 0 and 1. Therefore

$$\begin{aligned} \int_0^\infty J_0(zt)\,dt \int_0^1 \sin xt\,.\cos^{-1} x\,dx &= \int_z^1 \frac{\cos^{-1} x\,dx}{\sqrt{(x^2-z^2)}} \\ &= -\tfrac{1}{2}\pi \log z \qquad (0 < z < 1). \end{aligned}$$

Now $$\begin{aligned} \int_0^1 \sin xt\,.\cos^{-1} x\,dx &= \frac{\pi}{2t} - \frac{1}{t}\int_0^1 \frac{\cos xt}{\sqrt{(1-x^2)}}\,dx \\ &= \frac{\pi}{2t}\{1 - J_0(t)\}; \end{aligned}$$

therefore $$\int_0^\infty J_0(zt)\,\{1 - J_0(t)\}\,\frac{dt}{t} = -\log z \qquad (z < 1).$$

---

* This follows from the fact that the integrals

$$\int_0^m \frac{\sin h\,(u+z)}{u+z}\,g(z)\,dz, \qquad \int_0^m \frac{\sin h\,(u-z)}{u-z}\,g(z)\,dz$$

tends *uniformly* towards the values 0 and $g(u)$ as $h \to \infty$. (E. W. Hobson, "A general convergence theorem," *Proc. London Math. Soc.*, ser. 2, vol vi., p 349.)

† Weber, *l.c.*

The case in which $z>1$ may be deduced from this by putting $t=x/z$, $z=1/y$; for by Frullani's theorem

$$\int_0^\infty \left\{J_0\left(\frac{x}{y}\right)-J_0(x)\right\}\frac{dx}{x}=-\log\frac{1}{y}.$$

Hence
$$\int_0^\infty J_0(zt)\{1-J_0(t)\}\frac{dt}{t}=-\log z \quad (z<1)$$
$$=0 \quad (z>1).$$

This result may also be deduced by Hankel's inversion formula from the equation

$$\int_0^1 J_0(zt)\log t\,.\,t\,dt=\frac{1}{z^2}\{J_0(z)-1\},$$

which is easily verified by integration by parts, for

$$tJ_0(zt)=-\frac{1}{z^2}\frac{d}{dt}\left\{t\frac{d}{dt}J_0(zt)\right\}.$$

5. The equation

$$\int_z^1\frac{\cos^{-1}x\,dx}{\sqrt{(x^2-z^2)}}=-\tfrac{1}{2}\pi\log z \quad (0<z<1)$$

may be established by means of Abel's inversion formula, for if

$$-\tfrac{1}{2}\pi\log z=\int_z^1\frac{\phi(x)\,dx}{\sqrt{(x^2-z^2)}},$$

the inversion formula gives

$$\phi(x)=\frac{d}{dx}\int_x^1\frac{\log z\,.\,z\,dz}{\sqrt{(z^2-x^2)}}.$$

Integrating by parts, we have

$$\phi(x)=-\frac{d}{dx}\int_x^1\sqrt{(z^2-x^2)}\frac{dz}{z}$$
$$=\int_x^1\frac{x\,dz}{z\sqrt{(z^2-x^2)}}=\left[\sec^{-1}\frac{z}{x}\right]_x^1$$
$$=\sec^{-1}\left(\frac{1}{x}\right)=\cos^{-1}.x.$$

NOTES ON SOME POINTS IN THE INTEGRAL CALCULUS.

By *G. H. Hardy.*

XXXIII.

Some cases of the inversion of the order of integration.

1. I HAVE discussed elsewhere,* for a special purpose, the question of the inversion of the order of integration expressed by the formula

$$(1) \qquad \int_{-\infty}^{\infty} \phi(x)\, dx \int_{-\infty}^{\infty} f(\lambda) \overset{\cos}{\underset{\sin}{\cdot}} \lambda x\, d\lambda$$
$$= \int_{-\infty}^{\infty} f(\lambda)\, d\lambda \int_{-\infty}^{\infty} \phi(x) \overset{\cos}{\underset{\sin}{\cdot}} \lambda x\, dx.$$

I proved there that the formula holds under a variety of conditions, which I will re-state.

THEOREM 1. *The inversion is legitimate if* (i) ϕ *and* f *are regularly integrable*† *in any finite intervals,* (ii) *the integrals*

$$\int_{-\infty}^{\infty} |\phi|\, dx, \quad \int_{-\infty}^{\infty} |f|\, d\lambda$$

are convergent.‡

This theorem is of course only a very special case of a general theorem due to de la Vallée-Poussin.§

THEOREM 2. *The inversion is legitimate if* (i) ϕ *and* f *are regularly integrable in any finite intervals,* (ii) *the integral*

$$\int_{-\infty}^{\infty} |\phi(x)|\, dx$$

is convergent, (iii) $\phi(x)$ *tends steadily to limits* $\phi(+0)$, $\phi(-0)$

* "Fourier's double integral and the theory of divergent integrals," *Camb. Phil. Trans.*, vol. xxi., p. 427. I refer to this paper as "F. I."

† *I.e.*, integrable and absolutely integrable; see "F. I," p. 427 (footnote) and p. 434.

‡ "F. I," p. 436.

§ Bromwich, *Infinite Series*, p. 457.

as $x \to 0$ *by positive or negative values*, (iv) $f(\lambda)$ *tends steadily to zero as* $\lambda \to \infty$ *or* $\lambda \to -\infty$, (v) *the integrals*

$$\int^{\infty} \frac{f(\lambda)}{\lambda} d\lambda, \quad \int_{-\infty} \frac{f(\lambda)}{\lambda} d\lambda$$

*are convergent.**

With regard to the conditions of this theorem it was to be remarked (*a*) that condition (v) is unnecessary in the case of the cosine integral, and (*b*) that condition (iv) may be replaced by the more general condition that $f(\lambda)$ *is of limited total fluctuation in intervals* $(-\infty, -l)$, (l, ∞)—a condition which will certainly be satisfied if $f'(\lambda)$ *exists and is absolutely integrable up to* ∞ *and down to* $-\infty$.

2. These sets of conditions were general enough for the end that I had in view. But the question is one which arises frequently in analysis, and I find that there are simple and interesting applications which require more general conditions. I propose, therefore, in this and a subsequent note, to state and illustrate some additional theorems. The conditions of these theorems are framed with an eye to applications, and make no pretence to a *maximum* of generality.

3. In the theorems which follow I suppose, for the sake of simplicity of statement, that the range of integration with respect to each variable is $(0, \infty)$. There is, of course, no difficulty in modifying the enunciations so as to apply to a range infinite both ways. The first two theorems apply only to the integral which contains $\sin \lambda x$.

THEOREM 3. *The inversion is legitimate, in the case of the sine-integral, if* (i) $\phi(x)$ *is regularly integrable throughout any finite interval*, (ii) $f(\lambda)$ *is regularly integrable throughout any finite interval which does not include* $\lambda = 0$, (iii) $f(\lambda)$ *may be expressed, near* $\lambda = 0$, *in the form* $\lambda^{-1-s} F(\lambda)$, *where* $0 \leq s < 1$ *and* $F(\lambda)$ *tends steadily to a limit* $F(+0)$ *as* $\lambda \to 0$, (iv) *the integrals*

$$\int_0^{\infty} x^s |\phi| \, dx, \quad \int_{\lambda_0}^{\infty} |f| \, d\lambda \quad (\lambda_0 > 0)$$

are convergent.

* "F. I," p. 437: the theorem there is stated for intervals of integration $(0, \infty)$ instead of $(-\infty, \infty)$. It is, of course, to be understood that $\phi(x)$ and $f(\lambda)$ need only be monotonic for sufficiently small values of x and sufficiently large values of λ.

THEOREM 4. *The inversion is legitimate if* (i) $f(\lambda)$ *satisfies conditions* (ii) *and* (iii) *of Theorem* 3, (ii) $\phi(x)$ *satisfies similar conditions* (*with* r *instead of* s), (iii) *the integrals*

$$\int_{x_0}^{\infty} x^s |\phi| \, dx \quad (x_0 > 0), \quad \int_{\lambda_0}^{\infty} \lambda^r |f| \, d\lambda \quad (\lambda_0 > 0)$$

are convergent.

It will be noted that if (*e.g.*) $f(\lambda)$ is of the form $F(\lambda)/\lambda$ in the neighbourhood of the origin (so that $s=0$), the condition imposed on $\phi(x)$ in these theorems, as regards its behaviour at infinity, is identical with that of Theorem 1.

These theorems are extensions of Theorem 1. As an extension of Theorem 2, we have the following theorem (applying to both the sine and cosine integrals).

THEOREM 5. *The inversion is legitimate if* (i) ϕ *satisfies conditions* (i) *and* (ii) *of Theorem* 2, (ii) f *satisfies conditions* (i) *and* (iv) *of Theorem* 2,* (iii) ϕ *can be expressed, near* $x=0$, *in the form* $x^{-s}\psi(x)$, *where* $0 \leqq s < 1$, *and* $\psi(x)$ *tends steadily to a limit* $\psi(+0)$ *as* $x \rightarrow 0$, (iv) *the integral*

$$\int^{\infty} \frac{f(\lambda)}{\lambda^{1-s}} \, d\lambda$$

s convergent.

These three theorems can all be proved by a modification of the arguments used in my former paper. I shall content myself with showing this in the case of Theorem 5.

4. We proceed exactly as in the proof of Theorem 2,† until we come to the last stage, where we have to prove that

$$(2) \qquad \int_0^{x_0} \frac{\psi(x)}{x^s} \, dx \int_l^{\infty} f(\lambda) \cos \lambda x \, d\lambda$$

is convergent and tends to zero as $l \rightarrow \infty$. I prove this first in the special case in which $\psi(x)$ is replaced by unity. We have

$$(3) \qquad \int_{\xi}^{x_0} \frac{dx}{x^s} \int_l^{\infty} f(\lambda) \cos \lambda x \, d\lambda = \int_l^{\infty} f(\lambda) \, d\lambda \int_{\xi}^{x_0} \frac{\cos dx}{\lambda^s} \, dx.$$

* Naturally only in so far as *positive* values of x and λ are concerned.
† "F. I," p. 438. The same argument applies to the sine-integral.

for $0 < \xi < x_0$. This equation will still hold for $\xi = 0$ if

$$\int_l^\infty f(\lambda)\, d\lambda \int_0^\xi \frac{\cos \lambda x}{x^s}\, dx$$

is convergent and tends to zero as $\xi \to 0$, or if this is true of

$$(4) \qquad \int_l^\infty \frac{f(\lambda)}{\lambda^{1-s}}\, d\lambda \int_0^{\lambda\xi} \frac{\cos u}{u^s}\, du.$$

Now $\int_0^{\lambda\xi} \frac{\cos u}{u^s}\, du$ is a continuous function of λ and ξ, and ess in absolute value than an absolute constant K. It follows hat (4) is convergent and uniformly convergent throughout in interval of values of ξ including the value 0. It therefore tends to zero as $\xi \to 0$. Hence

$$(5) \quad \int_0^{x_0} \frac{dx}{x^s} \int_l^\infty f(\lambda) \cos \lambda x\, d\lambda = \int_l^\infty f(\lambda)\, d\lambda \int_0^{x_0} \frac{\cos \lambda x}{x^s}\, dx.$$

It follows, by the second mean value theorem, that the tntegral (2) is convergent and equal to

$$\psi(+0) \int_0^{x_1} \frac{dx}{x^s} \int_l^\infty f(\lambda) \cos \lambda x\, d\lambda + \psi(x_0) \int_{x_1}^{x_0} \frac{dx}{x^s} \int_l^\infty f(\lambda) \cos \lambda x\, d\lambda^*$$

$$= \psi(+0) \int_l^\infty \frac{f(\lambda)}{\lambda^{1-s}}\, d\lambda \int_0^{\lambda x_1} \frac{\cos u}{u^s}\, du + \psi(x_0) \int_l^\infty \frac{f(\lambda)}{\lambda^{1-s}}\, d\lambda \int_{\lambda x_1}^{\lambda x_0} \frac{\cos u}{u^s}\, du,$$

where $0 < x_1 < x_0$. But this is plainly less in absolute value than a constant multiple of $\int_l^\infty \frac{f(\lambda)}{\lambda^{1-s}}\, d\lambda$,† and so tends to zero as $l \to \infty$. This completes the proof of Theorem 5.

It might be thought that there was room, in the case of the *sine* integral, for a further generalisation of Theorem 2, in which $\phi(x)$ or $f(\lambda)$ should behave, near $x = 0$ or $\lambda = 0$, like x^{-1-r} or λ^{-1-s}. A little consideration shows that, for practical purposes, there is only one such case of importance. If $\phi(x)$ had the form suggested, we should have to impose on $f(\lambda)$ a condition, viz., the convergence of $\int^\infty \lambda^r f(\lambda)\, d\lambda$, which cannot possibly be satisfied unless $\int^\infty f(\lambda)\, d\lambda$ is convergent. And when $f(\lambda)$ has the form suggested it usually happens, in cases of interest, that $\int^\infty f(\lambda)\, d\lambda$ is convergent,

* If ψ has an ordinary discontinuity for $x = x_0$ (as is consistent with the conditions), we must replace $\psi(x_0)$ by $\psi(x_0 - 0)$.

† $f(\lambda)$, being ultimately monotonic, is of course ultimately of constant sign we may suppose this sign positive.

so that it is hardly necessary to frame a general theorem to meet this case. The exception to these remarks arises when $s=0$, so that $f(\lambda)$, near the origin, is of the form $F(\lambda)/\lambda$, where $F(\lambda)$ is monotonic. This case is of some importance. Suppose, for example, that the subject of integration is

$$e^{-x}\frac{\sin\lambda x}{\lambda}.$$

Integration, first with respect to x, gives

$$\int_0^\infty \frac{d\lambda}{1+\lambda^2}=\tfrac{1}{2}\pi.$$

Integration, first with respect to λ, gives

$$A\int_0^\infty e^{-x}\,dx=A,$$

where $$A=\int_0^\infty \frac{\sin u}{u}\,du.$$

Thus, if the inversion of the order of integration can be justified, we see that $A=\frac{1}{2}\pi$. But, as neither of the integrals

$$\int_0 \frac{d\lambda}{\lambda},\quad \int^\infty \frac{d\lambda}{\lambda}$$

is convergent, we cannot justify the inversion either by Theorem 2 or by Theorem 3. This case is met by

THEOREM 6. *The inversion is legitimate, in the case of the sine integral, if the conditions of Theorem 2 or of Theorem 5 are satisfied, except that, near* $\lambda=0$,

$$f(\lambda)=F(\lambda)/\lambda,$$

where $F(\lambda)$ *tends steadily to a limit as* $\lambda\to 0$.*

The reasoning by which this result is established is of precisely the same character as that already used, and I need not write out a proof.

5. The theorems which precede may all be generalised by supposing the integrals (1) to contain, instead of $\cos\lambda x$ or $\sin\lambda x$, a general function $\theta(\lambda x)$ subject to appropriate restrictions. Thus Theorem 1 holds if $\theta(u)$ is any con-

tinuous function whose modulus has a finite upper limit; and Theorem 5 holds if we suppose in addition that

$$\int^{u} \theta(v)\, dv$$

oscillates at most finitely. This includes (for $s=0$) the corresponding generalisation of Theorem 2. Finally, Theorems 3, 4, and 6 hold if $\theta(u)$ vanishes to the first order for $u=0$ (*i.e.*, if $\theta(u) = u\Theta(u)$, where Θ is continuous for $u=0$). If, more generally, we suppose $\theta(u) = u^t\Theta(u)$, we must suppose r and s less than t.† All these conclusions follow without any serious change in the arguments we have used.

6. I proceed now to give some illustrations of the use of Theorems 1–5. The only difficulty is to make a selection from the large number that suggest themselves.

(α) Let

$$I(s) = \int_0^\infty x^{s-1} \cos x\, dx, \quad J(s) = \int_0^\infty x^{s-1} \sin x\, dx,$$

$$K(s) = \int_0^\infty \frac{x^{s-1}}{1+x}\, dx.$$

Then

$$\Gamma(1-s)\, I(s) = \int_0^\infty e^{-x}\, dx \int_0^\infty \lambda^{s-1} \cos \lambda x\, d\lambda$$

$$= \int_0^\infty \frac{\lambda^{s-1}\, d\lambda}{1+\lambda^2} = \tfrac{1}{2} \int_0^\infty \frac{\mu^{\frac{1}{2}s-1}\, d\mu}{1+\mu} = \tfrac{1}{2} K\left(\tfrac{1}{2}s\right)$$

if $0 < s < 1$. The inversion here is justified by Theorem 2. Again

$$\Gamma(1-s)\, J(s) = \int_0^\infty e^{-x}\, dx \int_0^\infty \lambda^{s-1} \sin \lambda x\, d\lambda$$

$$= \int_0^\infty \frac{\lambda^{s}\, d\lambda}{1+\lambda^2} = \tfrac{1}{2} \int_0^\infty \frac{\mu^{\frac{1}{2}(s-1)}}{1+\mu}\, d\mu = \tfrac{1}{2} K\left\{\tfrac{1}{2}(1+s)\right\}$$

if $-1 < s < 1$. The inversion here is justified by Theorem 2 if $0 < s < 1$, by Theorem 3 if $-1 < s < 0$, and by Theorem 6 if $s = 0$. Finally

$$\Gamma(s)\,\Gamma(1-s) = \int_0^\infty e^{-x}\, dx \int_0^\infty e^{-\lambda x} \lambda^{s-1}\, d\lambda = \int_0^\infty \frac{\lambda^{s-1}}{1+\lambda}\, d\lambda = K(s),$$

if $0 < s < 1$. Here we may appeal to de la Vallée-Poussin's

---

* Or $\lambda \to -0$ in the case of Theorem 2.

† These statements seem sufficiently general for ordinary purposes; there would of course be no difficulty in extending them further.

standard theorem. We thus obtain the values of $I(s)$, $J(s)$, and $K(s)$, in all cases in which they are convergent, in terms of gamma-functions: if we use the formula

$$\Gamma(s)\,\Gamma(1-s) = \pi \operatorname{cosec} s\pi,$$

or evaluate $K(s)$ independently, we obtain the ordinary forms of the values of the integrals.

(β) In this example I shall assume that we know the values of the integrals

$$\int_0^\infty e^{-x} x^{r-1} \begin{smallmatrix}\cos\\ \sin\end{smallmatrix} \lambda x\, dx = \frac{\Gamma(r)}{(1+\lambda^2)^{\frac{1}{2}r}} \begin{smallmatrix}\cos\\ \sin\end{smallmatrix} (r \arctan \lambda),$$

where $r > 0$ for the cosine integral, and $r > -1$ for the sine integral.

Now let us take

$$e^{-x} x^{r-1} \lambda^{s-1} \cos \lambda x,$$

where $r > 0$, $0 < s < 1$, and integrate from 0 to ∞ with respect to each variable. Integrating first with respect to λ, we obtain

$$\Gamma(s) \cos \tfrac{1}{2} s\pi \int_0^\infty e^{-x} x^{r-s-1}\, dx = \Gamma(s)\,\Gamma(r-s) \cos \tfrac{1}{2} s\pi,$$

provided $r > s$. Integrating first with respect to x, we obtain

$$\Gamma(r) \int_0^\infty \frac{\lambda^{s-1}}{(1+\lambda^2)^{\frac{1}{2}r}} \cos(r \arctan \lambda)\, d\lambda$$

$$= \Gamma(r) \int_0^{\frac{1}{2}\pi} (\cos\phi)^{r-s-1} (\sin\phi)^{s-1} \cos r\phi\, d\phi,$$

again provided $r > s$. Hence we are led to the formula

$$\int_0^{\frac{1}{2}\pi} (\cos\phi)^{r-s-1} (\sin\phi)^{s-1} \cos r\phi\, d\phi = \frac{\Gamma(s)\,\Gamma(r-s)}{\Gamma(r)} \cos \tfrac{1}{2} s\pi,$$

holding for $r > s$, $0 < s < 1$.* The inversion of the order of integration is justified by Theorem 5, since $\int^\infty \lambda^{s-r-1} d\lambda$ is convergent if $r > s$.

If we take

$$e^{-x} x^{r-1} \lambda^{s-1} \sin \lambda x$$

as the subject of integration, where $r > s$, $-1 < s < 1$, we obtain, in the same way, the formula

$$\int_0^{\frac{1}{2}\pi} (\cos\phi)^{r-s-1} (\sin\phi)^{s-1} \sin r\phi\, d\phi = \frac{\Gamma(s)\,\Gamma(r-s)}{\Gamma(r)} \sin \tfrac{1}{2} s\pi.$$

If $0 < s < 1$ (in which case also $r > 0$), the inversion is justified by Theorem 5. If $-1 < s < 0$ and $r > 0$, it is justified by Theorem 3; and if $s = 0$, $r > 0$ by Theorem 6. Finally, if $-1 < s < r \leqq 0$, it is justified by Theorem 4, since

$$\int^{\infty} e^{-x} x^{r-s-1} dx, \quad \int^{\infty} \lambda^{s-r-1} d\lambda$$

are convergent.†

(γ) Let us take as our subject of integration

$$\lambda^{s-1} \operatorname{sech} \pi x \cos \lambda x \quad (0 < s < 1).$$

Using Theorem 2, we obtain

$$\tfrac{1}{2} \int_0^{\infty} \frac{\lambda^{s-1}}{\cosh \frac{1}{2}\lambda} d\lambda = \Gamma(s) \cos \tfrac{1}{2} s\pi \int_0^{\infty} \frac{x^{-s}}{\cosh \pi x} dx.$$

If we put $\lambda = 2\xi$ on the left-hand side and $\pi x = \xi$ on the right-hand side, and observe that

$$\tfrac{1}{2} \int_0^{\infty} \frac{\xi^{s-1}}{\cosh \xi} d\xi = \Gamma(s) \left(\frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \dots \right) = \Gamma(s)\, \eta(s),$$

say, we obtain the formula

$$\eta(1-s) = \Gamma(s) \left(\tfrac{1}{2}\pi\right)^{-s} \sin \tfrac{1}{2} s\pi\, \eta(s).‡$$

7. There are still a variety of interesting questions to consider. We have supposed so far either (i) that $f(\lambda)$ is absolutely integrable up to ∞ or (ii) that $f(\lambda)$ is ultimately monotonic. We must consider next the case in which $f(\lambda)$ is the product of $F(\lambda)$ by an oscillating factor such as $\cos a\lambda$ or $\sin a\lambda$, $F(\lambda)$ being subject to (ii), but not to (i). There are also interesting cases in which neither $f(\lambda)$ nor $\phi(x)$ is absolutely integrable up to ∞. I shall return to these questions in another note.

---

* This formula was first given by Kummer; see Dirichlet-Meyer, *Bestimmte Integrale*, p. 224.

† The theorems give between them the *exact* ranges of r and s, for which the transformations are valid. The ultimate formulæ hold for wider ranges; in fact, the inequality $s < 1$ is superfluous. But this shows, not that the theorems do not give complete information about the inversion of integrations, but that the ultimate formulæ hold in cases in which the inversion is *not* legitimate. There is no difficulty in extending the formulæ to their full range by means of elementary reduction formulæ.

‡ See Bromwich, *Infinite Series*, p. 491. The formula is originally due to Schlömilch: see his *Compendium der höheren Analysis*, vol. ii., p. 286. It is of course analogous to the functional equation satisfied by $\zeta(s)$.

SUBSTITUTIONS PERMUTABLE WITH A CANONICAL SUBSTITUTION.

By *Harold Hilton.*

§ 1. THE properties of substitutions permutable with a given substitution have been discussed by various authors. The following elementary methods of arriving at some of the results they have obtained may be of interest.

Any homogeneous linear substitution of degree m may be transformed into the *canonical* form S:

$$x_1' = \lambda_1 x_1 + \beta_1 x_2, \quad x_2' = \lambda_2 x_2 + \beta_2 x_3,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots,$$
$$x'_{m-1} = \lambda_{m-1} x_{m-1} + \beta_{m-1} x_m, \quad x'_m = \lambda_m x_m,$$

where $\beta_t = 0$ or 1, and is always 0 if $\lambda_t \neq \lambda_{t+1}$.*

Let A denote a substitution

$$x_t' = a_{t1} x_1 + a_{t2} x_2 + \dots + a_{tm} x_m \quad (t = 1, 2, \dots, m)$$

permutable with S.

Equating the elements in the i^{th} row and j^{th} column of the matrices of AS and SA, we have

$$a_{i,j}\lambda_j + a_{i,j-1}\beta_{j-1} = a_{i,j}\lambda_i + a_{i+1,j}\beta_i \dots\dots\dots\dots\dots\dots (\alpha)$$

or

$$\left.\begin{aligned} a_{1,j}(\lambda_1 - \lambda_j) &= a_{1,j-1}\beta_{j-1} - a_{2,j}\beta_1 \\ a_{2,j}(\lambda_2 - \lambda_j) &= a_{2,j-1}\beta_{j-1} - a_{3,j}\beta_2 \\ &\vdots \\ a_{m-1,j}(\lambda_{m-1} - \lambda_j) &= a_{m-1,j-1}\beta_{j-1} - a_{m,j}\beta_{m-1} \\ a_{m,j}(\lambda_m - \lambda_j) &= a_{m,j-1}\beta_{j-1} \end{aligned}\right\} \dots\dots (\alpha').$$

Suppose now, for example,

$$\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4, \ \beta_1 = \beta_2 = \beta_3 = 1, \ \beta_4 = 0; \quad \text{but } \lambda_1 \neq \lambda_5, \lambda_6, \dots .$$

The equations (α') give (taking $j = 5, 6, \dots$)

$$\left.\begin{aligned} a_{15}(\lambda_1 - \lambda_5) &= -a_{25} \\ a_{25}(\lambda_1 - \lambda_5) &= -a_{35} \\ a_{35}(\lambda_1 - \lambda_5) &= -a_{45} \\ a_{45}(\lambda_1 - \lambda_5) &= \ \ 0 \end{aligned}\right\}, \qquad \left.\begin{aligned} a_{16}(\lambda_1 - \lambda_6) &= a_{15}\beta_5 - a_{26} \\ a_{26}(\lambda_1 - \lambda_6) &= a_{25}\beta_5 - a_{36} \\ a_{36}(\lambda_1 - \lambda_6) &= a_{35}\beta_5 - a_{46} \\ a_{46}(\lambda_1 - \lambda_6) &= a_{45}\beta_5 \end{aligned}\right\}, \dots,$$

whence

$$a_{15} = a_{25} = a_{35} = a_{45} = 0, \ a_{16} = a_{26} = a_{36} = a_{46} = 0, \ \dots .$$

---

* *Mess. Math*, vol. 39 (1909), p. 21.

The method is general, and gives us at once

$$a_{ij}=0 \text{ whenever } \lambda_i \neq \lambda_j \text{ .... } (\beta).$$

If $\lambda_i=\lambda_j$, we have from (α)

$$a_{i,j-1}\beta_{j-1}=a_{i+1,j}\beta_i.$$

Hence

$$\left.\begin{array}{lll} a_{i,j-1}=a_{i+1,j} & \text{when} & \beta_i=1,\ \beta_{j-1}=1 \\ a_{i,j-1}=0 & \text{when} & \beta_i=0,\ \beta_{j-1}=1 \\ a_{i+1,j}=0 & \text{when} & \beta_i=1,\ \beta_{j-1}=0 \end{array}\right\} \text{......} (\beta').$$

Apply (β') to the case in which S has the matrix

$$\begin{vmatrix} \alpha & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha \end{vmatrix} \text{................} (\gamma),$$

and we readily see that A has a matrix of the form

$$\begin{vmatrix} a & a' & a'' & f & f' & f'' & g & g' & h & h' & i & i' \\ 0 & a & a' & 0 & f & f' & 0 & g & 0 & h & 0 & i \\ 0 & 0 & a & 0 & 0 & f & 0 & 0 & 0 & 0 & 0 & 0 \\ q & q' & q'' & b & b' & b'' & j & j' & k & k' & l & l' \\ 0 & q & q' & 0 & b & b' & 0 & j & 0 & k & 0 & l \\ 0 & 0 & q & 0 & 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & r & r' & 0 & s & s' & c & c' & m & m' & n & n' \\ 0 & 0 & r & 0 & 0 & s & 0 & c & 0 & m & 0 & n \\ 0 & t & t' & 0 & u & u' & v & v' & d & d' & p & p' \\ 0 & 0 & t & 0 & 0 & u & 0 & v & 0 & d & 0 & p \\ 0 & w & w' & 0 & x & x' & y & y' & z & z' & e & e' \\ 0 & 0 & w & 0 & 0 & x & 0 & y & 0 & z & 0 & e \end{vmatrix} \text{...........} (\delta).$$

As another example apply (β), (β') to the case in which S has the matrix

$$\begin{vmatrix} \alpha & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \beta & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \beta & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \gamma \end{vmatrix},$$

then A has the matrix

$$\begin{vmatrix} a & a' & e & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & f & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c & c' & c'' & 0 \\ 0 & 0 & 0 & 0 & c & c' & 0 \\ 0 & 0 & 0 & 0 & 0 & c & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & d \end{vmatrix} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (\epsilon).$$

From these two examples the law of formation of the coefficients of A in the general case is also evident.*

If, in S, $\lambda_1 = \lambda_2 = \lambda_3 = \ldots$, β_r, β_{r+s}, β_{r+s+t}, ... are zero, and the other β's are unity ($r \geq s \geq t \geq \ldots$), then the invariant-factors of S are readily seen to be

$$(\lambda - \lambda_1)^r,\ (\lambda - \lambda_1)^s,\ (\lambda - \lambda_1)^t,\ (\lambda - \lambda_1)^u, \ldots .$$

From the example (δ), the number of arbitrary constants in A is clearly

$$(r + s + t + u + \ldots) + 2\,(s + 2t + 3u + \ldots) = (r + 3s + 5t + 7u + \ldots).$$

Hence we have the well-known result:—

"If the exponents of the invariant-factors, corresponding to any characteristic-root† of a given substitution, are r, s, t, u, ..., the number of linearly independent substitutions permutable with it is

$$\Sigma\,(r + 3s + 5t + 7u + \ldots),$$

the summation being extended over each distinct characteristic-root."‡

§ 2. Consider now the case in which S has a single invariant-factor, *i.e.*, S takes the form

$$x_1' = \alpha x_1 + x_2,\ x_2' = \alpha x_2 + x_3,\ \ldots,\ x'_{m-1} = \alpha x_{m-1} + x_m,\ x'_m = \alpha x_m.$$

Then A takes the form

$$x_1' = a x_1 + a' x_2 + a'' x_3 + \ldots + a^{(m-1)} x_m,$$
$$x_2' = a x_2 + a' x_3 + \ldots + a^{(m-2)} x_m,\ \ldots,\ x'_m = a x_m.$$

We prove at once by induction that A^n is

$$x_1' = p x_1 + p' x_2 + p'' x_3 + \ldots + p^{(m-1)} x_m,$$
$$x_2' = p x_2 + p' x_3 + \ldots + p^{(m-2)} x_m,\ \ldots,\ x'_m = p x_m,$$

where

$$p + p'x + p''x^2 + \ldots \equiv (a + a'x + a''x^2 + \ldots + a^{(m-1)} x^{m-1})^n.$$

---

* An equivalent result is given by Hensel, *Crelle*, 127 (1904), p. 158.

† *I.e.*, a root of the characteristic equation of the given substitution.

‡ See, for instance, Frobenius, *Berliner Sitzungsberichte* (1910), p. 3.

It follows that A is only finite if it is the similarity

$$x_1' = ax_1,\ x_2' = ax_2,\ \ldots,\ x'_m = ax_m,$$

where a is a root of unity.

The poles of A are $(X_1, X_2, \ldots, X_r, 0, 0, \ldots, 0)$* when $a' = a'' = a''' = \ldots = a^{(r-1)} = 0$, $a^{(r)} \neq 0$; the ratios $X_1 : X_2 : \ldots : X_r$ being arbitrary. There are therefore r invariant-factors of A. It is not hard to calculate these invariant-factors for values of m up to 8,† but they do not appear to satisfy any simple general law.

If A is of finite order, there must be an $(m-1)$-ply infinite number of poles, and therefore $a' = a'' = \ldots = a^{(r-1)} = 0$ as before obtained.

Remembering that S^t is

$$x_1' = \alpha^t x_1 + {}^tC_1 \alpha^{t-1} x_2 + {}^tC_2 \alpha^{t-2} x_3 + \ldots,$$

$$x_2' = \alpha^t x_2 + {}^tC_1 \alpha^{t-1} x_3 + {}^tC_2 \alpha^{t-2} x_3 + \ldots,\ \ldots,\ x'_m = \alpha^t x_m,$$

we have $\quad A \equiv k_0 S^0 + k_1 S^1 + k_2 S^2 + \ldots + k_{m-1} S^{m-1}$

if

$$a\ = k_0 + k_1\alpha + k_2\alpha^2 + k_3\alpha^3 + \ldots + k_{m-1}\alpha^{m-1},$$

$$a' = k_1 + k_2\,{}^2C_1\alpha + k_3\,{}^3C_1\alpha^2 + \ldots + k_{m-1}\,{}^{m-1}C_1\alpha^{m-2},$$

$$a'' = k_2 + k_3\,{}^3C_2\alpha + \ldots + k_{m-1}\,{}^{m-1}C_2\alpha^{m-3},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a^{(m-1)} = k_{m-1}.$$

Values of $k_0, k_1, \ldots, k_{m-1}$ can always be found which will satisfy these relations.

Even if S had more than one invariant-factor, the matrix of $k_0 S^0 + k_1 S^1 + k_2 S^2 + \ldots$ would have no non-zero term to the left of its leading diagonal; but this is no longer true of the general substitution permutable with S. Hence we have Cecioni's result‡ that "Every substitution permutable with a given substitution P is a linear aggregate of powers of P if, and only if, a single invariant-factor of P corresponds to each distinct characteristic-root of P."

§ 3. Let us now return to the case in which the given canonical substitution has any invariant-factors.

---

* For the notation, see Hilton's *Finite Groups*, chap. III.

† *E.g.*, for $m = 8$, the exponents of the invariant-factors when $r = 1, 2, 3, \ldots$ are respectively (8), (4, 4), (3, 3, 2), (2, 2, 2, 2), (2, 2, 2, 1, 1), (2, 2, 1, 1, 1, 1), (2, 1, 1, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1, 1, 1).

‡ *Atti Reale Accad. dei Lincei*, 18 (1909), p. 566.

The determinant of the general substitution permutable with S can readily be factorized. For example, the determinant (δ) is

$$\begin{vmatrix} a & f \\ q & b \end{vmatrix}^3 \times \begin{vmatrix} c & m & n \\ v & d & p \\ y & z & e \end{vmatrix}^2 .$$

This may be proved by rearranging columns and rows in (δ) so that the columns (and rows) now in the order 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 are in the order 1, 4, 2, 5, 3, 6, 7, 9, 11, 8, 10, 12.

The characteristic determinant of (δ) is obtained by changing a, b, c, d, e into $a-\lambda$, $b-\lambda$, $c-\lambda$, $d-\lambda$, $e-\lambda$. Hence the characteristic equation of a substitution permutable with a given substitution P cannot have its roots all distinct unless all the invariant-factors of P are simple.

The poles of (δ) are $(X_1, 0, 0, X_2, 0, 0, 0, 0, 0, 0, 0, 0)$, where (X_1, X_2) is any pole of the substitution with matrix

$$\begin{vmatrix} a & f \\ q & b \end{vmatrix},$$

and $(0, 0, 0, 0, 0, 0, Y_1, 0, Y_2, 0, Y_3, 0)$, where (Y_1, Y_2, Y_3) is any pole of the substitution with matrix

$$\begin{vmatrix} c & m & n \\ v & d & p \\ y & z & e \end{vmatrix}.$$

There will, in general, be no other poles of (δ) unless certain relations hold between the elements of (δ).

These results are at once generalized.

§ 4. The substitution with matrix

$$\begin{vmatrix}
a & a' & a'' & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a & a' & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & a & a' & a'' & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & a & a' & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & a & a' & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a' & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a' \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a
\end{vmatrix} \quad \ldots\ldots\ldots\ldots(\zeta)$$

is permutable with *every* substitution of the form (δ). That any substitution permutable with *every* substitution, whose

matrix is of the form (δ), has a matrix of the type (ζ) is proved as follows:—

Firstly, any such substitution has a matrix of the form

$$\begin{vmatrix}
a & a' & a'' & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & a & a' & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & b & b' & b'' & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & b & b' & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & c & c' & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & c' & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d & d' & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & e & e' \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & e
\end{vmatrix} \quad \ldots\ldots\ldots\ldots\ldots(\eta),$$

for it is permutable with the canonical substitution of matrix

$$\begin{vmatrix}
\lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mu & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \mu & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mu & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \nu & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \nu & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \rho & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \rho & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sigma & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sigma
\end{vmatrix},$$

which is a particular case of (δ).

Again, if (η) is permutable with the substitution of matrix

$$\begin{vmatrix}
a & a' & a'' & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & a & a' & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & a & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & b & b' & b'' & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & b & b' & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & c & c' & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & c & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d & d' & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & d & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & e & e' \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & e
\end{vmatrix},$$

which is a particular case of (δ), we have

$$\mathrm{a}=\mathrm{b}=\mathrm{c}=\mathrm{d}=\mathrm{e},\quad \mathrm{a}'=\mathrm{b}'=\mathrm{c}'=\mathrm{d}'=\mathrm{e}',\quad \mathrm{a}''=\mathrm{b}''.$$

The result is at once generalized. A similar result was obtained by Autonne in another way.*

§5. Given two permutable substitutions, we can transform them so that one is in canonical form

$$\left.\begin{array}{l} x_1'=\lambda x_1+\beta_1 x_2,\ x_2'=\lambda x_2+\beta_2 x_3,\ \ldots,\ x'=\lambda x_r \\ x'_{r+1}=\mu x_{r+1}+\beta_{r+1}x_{r+2},\ \ldots,\ x'_{r+s}=\mu x_{r+s} \\ x'_{r+s+1}=\nu x_{r+s+1}+\beta_{r+s+1}x_{r+s+2},\ \ldots,\ x'_{r+s+t}=\nu x_{r+s+t},\ \ldots \end{array}\right\}\ldots(\theta),$$

where the β's are all 1 or 0, and no two of the quantities λ, μ, ν, ... are equal; and the other is the direct product of a substitution on $x_1, x_2, \ldots, x_r$, all of whose characteristic-roots are equal; a substitution on $x_{r+1}, x_{r+2}, \ldots, x_{r+s}$, all of whose characteristic-roots are equal; and so on.

As a simple example of the method, suppose that when one is transformed into canonical form it has the matrix

$$\left|\begin{array}{cccccc} \alpha & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & 0 & 0 & \alpha \end{array}\right|,$$

and the matrix of the other becomes

$$\left|\begin{array}{cccccc} a & a' & a'' & c & c' & c'' \\ 0 & a & a' & 0 & c & c' \\ 0 & 0 & a & 0 & 0 & c \\ d & d' & d'' & b & b' & b'' \\ 0 & d & d' & 0 & b & b' \\ 0 & 0 & d & 0 & 0 & b \end{array}\right|,$$

whose characteristic equation is

$$\left|\begin{array}{cc} a-\lambda & c \\ d & b-\lambda \end{array}\right|^3=0.$$

* *Journal de l'école Polytechnique*, II., 14 (1910), p. 125.

If the roots of this equation are not all equal, transform the substitutions by a substitution of matrix

$$\begin{vmatrix} l & 0 & 0 & n & 0 & 0 \\ 0 & l & 0 & 0 & n & 0 \\ 0 & 0 & l & 0 & 0 & n \\ p & 0 & 0 & m & 0 & 0 \\ 0 & p & 0 & 0 & m & 0 \\ 0 & 0 & p & 0 & 0 & m \end{vmatrix},$$

where l, m, n, p are chosen so that

$$x_3' = lx_3 + nx_6, \quad x_6' = px_3 + mx_6$$

transforms $\quad x_3' = ax_3 + cx_6, \quad x_6' = dx_3 + bx_6$

into a multiplication. The matrices of the two substitutions will now have the form

$$\begin{vmatrix} \alpha & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & 0 & 0 & \alpha \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} \mathrm{a} & \mathrm{a}' & \mathrm{a}'' & 0 & \mathrm{c} & \mathrm{c}' \\ 0 & \mathrm{a} & \mathrm{a}' & 0 & 0 & \mathrm{c} \\ 0 & 0 & \mathrm{a} & 0 & 0 & 0 \\ 0 & \mathrm{d} & \mathrm{d}' & \mathrm{b} & \mathrm{b}' & \mathrm{b}'' \\ 0 & 0 & \mathrm{d} & 0 & \mathrm{b} & \mathrm{b}' \\ 0 & 0 & 0 & 0 & 0 & \mathrm{b} \end{vmatrix},$$

where $\mathrm{a} \neq \mathrm{b}$.

Now transform by putting

$$x_1 = y_1 + \frac{\mathrm{c}}{\mathrm{b} - \mathrm{a}} y_5, \quad x_2 = y_2 + \frac{\mathrm{c}}{\mathrm{b} - \mathrm{a}} y_6, \quad x_3 = y_3,$$

$$x_4 = \frac{\mathrm{d}}{\mathrm{a} - \mathrm{b}} y_2 + y_4, \quad x_5 = \frac{\mathrm{d}}{\mathrm{a} - \mathrm{b}} y_3 + y_5, \quad x_6 = y_6,$$

and the matrices take the form

$$\begin{vmatrix} \alpha & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & 0 & 0 & \alpha \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} \mathrm{a} & A' & A'' & 0 & 0 & C \\ 0 & \mathrm{a} & A' & 0 & 0 & 0 \\ 0 & 0 & \mathrm{a} & 0 & 0 & 0 \\ 0 & 0 & D & b & B' & B'' \\ 0 & 0 & 0 & 0 & b & B' \\ 0 & 0 & 0 & 0 & 0 & b \end{vmatrix}.$$

Now transform by putting

$$y_1 = z_1 + \frac{C}{\mathrm{b}-\mathrm{a}} z_6, \quad y_2 = z_2, \quad y_3 = z_3, \quad y_4 = \frac{D}{\mathrm{a}-\mathrm{b}} z_3 + z_4, \quad y_5 = z_5, \quad y_6 = z_6,$$

when the matrices take the form

$$\begin{vmatrix} \alpha & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & 0 & 0 & \alpha \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} \mathrm{a} & \mathfrak{A}' & \mathfrak{A}'' & 0 & 0 & 0 \\ 0 & \mathrm{a} & \mathfrak{A}' & 0 & 0 & 0 \\ 0 & 0 & \mathrm{a} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{b} & \mathfrak{B}' & \mathfrak{B}'' \\ 0 & 0 & 0 & 0 & \mathrm{b} & \mathfrak{B}' \\ 0 & 0 & 0 & 0 & 0 & \mathrm{b} \end{vmatrix}.$$

Now transform the second substitution into canonical form by a substitution with matrix of the type

$$\begin{vmatrix} p_{11} & p_{12} & p_{13} & 0 & 0 & 0 \\ p_{21} & p_{22} & p_{23} & 0 & 0 & 0 \\ p_{31} & p_{32} & p_{33} & 0 & 0 & 0 \\ 0 & 0 & 0 & p_{44} & p_{45} & p_{46} \\ 0 & 0 & 0 & p_{54} & p_{55} & p_{56} \\ 0 & 0 & 0 & p_{64} & p_{65} & p_{66} \end{vmatrix},$$

and the required transformation is completed.

We readily show now that given any number of mutually permutable substitutions, we can transform them so that one is in canonical form and the others are direct products of the kind referred to at the beginning of this section, a result due to Dickson.*

* *Quarterly Journal*, vol. xl. (1909), p. 171.

ON QUASI-MERSENNIAN NUMBERS.

By *Lt.-Col. Allan Cunningham, R.E.*, Fellow of King's College, London.

[The author is indebted to Mr. H. J. Woodall, A.R.C.Sc., for reading the Proof sheets, and for suggestions.]

1. *Quasi-Mersennians.* THE principal characteristic of *Mersenne's Numbers* (M_q), which are defined by

$$M_q = (2^q - 1), \text{ with } q \text{ prime} \quad \text{.........} (1),$$

is that they possess *no algebraic divisors.* It is proposed to apply the term *Quasi-Mersennian* to numbers (N_q) of the type

$$N_q = x^q - y^q, \text{ with } q \text{ prime, and } x - y = 1 \quad \text{.........} (2),$$

from the similar property that—except in a few special cases (Art. 14 *et seq.*)—they also have no algebraic divisors. These are the numbers studied in this Paper, with special reference to their factorisation. They are of course only a special case of the more general type

$$N_q = (x^q - y^q) \div (x - y), \text{ wherein } x - y = \text{integer, and } q \text{ is } odd \text{......} (2a);$$

and are therefore subject to all the Rules characterising the more general form (with slight modification) *e.g.*

$$N_q = 6mq + 1 \;\; always \quad \text{.........} (3),$$

$$= t^2 - qu^2 = T^2 - qxyU^2, \text{ when } q = 4k+1 \quad \text{.........} (3a),$$

$$= t^2 + qu^2 = T^2 + qxy\,U^2, \text{ when } q = 4k-1 \quad \text{.........} (3b),$$

$$= A^2 + 3B^2, \text{ when } N_q \text{ is prime} \quad \text{.........} (3c).$$

This type (N_q) really includes Mersenne's Numbers (1) as a special case ($x = 2$, $y = 1$); but this Paper deals only with the more general cases ($x > 2$, $y > 1$).

1*a*. *Notation.* Throughout this Paper—

p denotes a *prime*; q is a *prime* exponent.

ω means an *odd* number, ϵ means an *even* number.

2. *Factorisation of* N_q. The possibility of *complete factorisation* (*i.e.* into prime factors) of these numbers decreases rapidly with increase of the index (q): the following are the highest numbers of this kind which can be completely factorised by the existing large Factor-Tables (the upper limit of which is now 10,017,000).

$q=$	3	5	7	11	13	17
x,y	1827,1826	38,37	11,10	4,3	3,2	2,1
N_q	19.199.2647;	11.61.1741;	1499.6329;	23.174659;	53.29927;	131071;

Beyond these limits it becomes necessary to search for special divisors by methods explained below (Art. 4 to 12), or to investigate cases which are algebraically resolvable into factors (Art. 14 to 23*b*).

3. *Divisors, Linear Forms.* Euler's general Rule for numbers of the more general forms (2*a*) is here applicable—

Every prime divisor of N_q must be of form $p = 2\varpi q + 1$........(4).

Hence, certain Rules of exclusion are easily derived. If $a, b, c, \ldots$, be *different* primes, then

N_q may $\equiv 0$, (mod $p = 2^\kappa . a + 1$); but only if $a = q$...............(4*a*),

N_q may $\equiv 0$, (mod $p = 2^\kappa . ab + 1$); but only if a or $b = q$........(4*b*),

N_q may $\equiv 0$, (mod $p = 2^\kappa . Q + 1$); but only if $Q = 0$ mod q...(4*c*).

3*a*. *Non-divisors.* Result (4*a*) involves that—

No Fermat's *prime*, $F_n = (2^{2^n} + 1)$ can be a divisor of any N_q.....(4*d*).

4. *Quadratic Factors.* Divisors of the simple form $p = 2q + 1$ obey the following simple Rule

$N_q \equiv 0$ (mod $p = 2q + 1$), if $(x/p)_2$, $(y/p)_2$ both $= +1$, or both $= -1$...(5).

These two simple Rules have the advantage of being easily applied to primes of any magnitude without requiring the use of Tables.

Here follow some simple general forms of such prime divisors (p),

Conditions	$y = \eta^2$	$x = \xi^2$	$x \neq \xi^2$, $y \neq \eta^2$	
$p = 2q + 1 =$	$4x\varpi - 1$	$4y\varpi - 1$	$4xy\varpi - 1$	...........(6).

The above List of forms of such divisors is of course very incomplete: its only use is that the primes specified are easily recognised. Here follows a complete List of the *linear forms* of such prime divisors ($p = 2q + 1$) for all values of $x \not> 12$. Of course $p = 2q + 1$ involves $p = 4\varpi + 3$.

Condition	$x, y =$	2, 1	3, 2	4, 3	5, 4	6 to 8	9, 8	
$(x/p) = (y/p) = +1$	$p =$	$8\varpi - 1$	$24\varpi - 1$	$12\varpi - 1$	$20\varpi + 11, 19$	*v* infra	$8\varpi - 1$	...(6*a*).
$(x/p) = (y/p) = -1$	$p =$	.	$24\varpi - 5$	.	.		.	...(6*b*).

x, y	p, $[(x/p) = (y/p) = +1]$.	p, $[(x/p) = (y/p) = -1]$.
6, 5	$120\varpi + 19, 71, 91, 119$	$120\varpi + 7, 83, 103, 107$
7, 6	$168\varpi + 19, 47, 115, 139, 143, 167$	$168\varpi + 11, 79, 107, 127, 151, 155$
8, 7	$56\varpi + 31, 47, 55$	$56\varpi + 11, 43, 51$
10, 9	$40\varpi + 3, 27, 31, 39$	None
11, 10	$220\varpi + 39, 43, 79, 83, 107, 123, 151$	$220\varpi + 23, 47, 59, 91, 103, 179, 207$
12, 11	$132\varpi + 35, 83, 95, 107, 131$	$132\varpi + 31, 67, 91, 103, 115$

High composite N_q. The highest* composite numbers of this kind at present known (to the author) are shown below; along with their quadratic divisors (p).

x, y	q	p	x, y	q	p	x, y	q	p
3, 2;	67109051,	134218103	6, 5;	67108683,	134217367	6, 5;	67108623,	134217247

5. *Prime Divisor Chain.* There exist certain sequences, called Chains, of primes $p_0, p_1, p_2, \ldots$, such that, in relation to a certain "base" (a),

$$a^{p_r} \equiv +1, \text{ (mod } p_{r+1}), \text{ wherein } p_{r+1} = 2p_r + 1, \ [r = 0, 1, 2, \text{ \&c.}] \ldots\ldots\ldots (7),$$

and in some cases this relation holds for several bases $a, b, c, \ldots$, and in some cases the bases $a, b, c, \ldots$, may be *successive integers.* In this latter case each adjacent pair of $a, b, c, \ldots$, may be taken for the x, y of a Quasi-Mersennian (N_q), so as to form a group of the numbers N_q, wherein q takes the values $p_0, p_1, p_2, \ldots$, the x, y being the same in any one group of N_q, so that

$$x^{p_0} - y^{p_0} \equiv 0 \text{ (mod } p_1), \ x^{p_1} - y^{p_1} \equiv 0 \text{ (mod } p_2), \ x^{p_2} - y^{p_2} \equiv 0 \text{ (mod } p_3), \text{ \&c.} (7a).$$

Ex. The short Table below shows several such Prime-Chains with the values of some of the bases $a, b, c, \ldots$, for which the above chain-property holds through some part of the prime-chain:

p_0	p_1	p_2	p_3	p_4	p_5	Values of a, b, c, &c.
89,	179,	359,	719,	1439,	2879	
63419,	126839,	253679,	567359,	1014719,	2029439	1, 2, 3, 4, 5, 6; 8, 9, 10;
127139,	254279,	508559,	1017119,	2034239,	4068479	15, 16; 24, 25;

The above prime-chains, of six links each, are the longest known to the author. Shorter chains (of fewer links) exist in much higher numbers: the highest known to the author are

p_0	p_1	p_2	Values of a, b, c, &c.
25000031,	50000063,	100000127;	1, 2, 3, 4; 8, 9;
25000199,	50000399,	100000799;	1, 2, 3, 4, 5, 6; 8, 9, 10; 15, 16; 24, 25;

6. *Other Factors,* (Partial Rule). It is clear that p will be a divisor of N_q, *i.e.*

$$N_q \equiv 0 \text{ (mod } p = nq + 1), \text{ if } (x/p)_n, (y/p)_n \text{ both } = +1, \text{ or both } = -1 \ldots (8).$$

These conditions are *not necessary* (*i.e.* primes may be divisors which do not satisfy them); but, when satisfied, they are *sufficient* conditions.

Their practical use is limited to the few small values of n (viz. $n = 4, 6, 8, 12$) for which algebraic expressions for $(x/p)_n$

* The six High Primes (q, p), here quoted, were shown to be prime in the author's Papers "On the Determination of Successive High Primes," in the *Messenger of Mathematics*, Vol. XXXV., 1905, p. 186; and Vol. XLI., 1911, p. 4. Four of these numbers were printed wrong in Art. 32c, Vol. XLI.

have been formed, and is further (practically) limited to the few small bases (x or $y = 2, 3, 5, 7, 11$, or powers and products thereof) for which those expressions have been reduced to an arithmetically workable form: and they also require the aid of Tables* of the 2ic partitions $p = \mathrm{a}^2 + \mathrm{b}^2$, $p = \mathrm{c}^2 + 2\mathrm{d}^2$, $p = A^2 + 3B^2$. In such cases they have the advantage of being easily applied to primes of any magnitude (within the limits of the Tables).

7. *Quartic Divisors* (Special case). For prime divisors of the simple form $p = 4q + 1$ the above Rule (8) becomes

$$N_q \equiv 0 \pmod{p = 4q+1}, \text{ if } (x/p)_4, (y/p)_4 \text{ both } = +1, \text{ or both } = -1 \ldots (9).$$

Now $p = 4q+1$ involves $p = \mathrm{a}^2 + \mathrm{b}^2$ [a & $\frac{1}{2}$b *odd*], and $(2/p)_2 = -1$.

Also, *one* of x, y is odd, and *one* even, (since $x - y = 1$).

Let ξ, η be the *odd* factors of x, y respectively, and 2^κ the even factor of x or y, so that

$$\text{Either } x = \xi,\ y = 2^\kappa . \eta; \quad \text{or } x = 2^\kappa . \xi,\ y = \eta \ldots\ldots\ldots\ldots (10).$$

Now the criteria for $(K/p)_4 = +1$ or -1, where K is an *odd* number (in the present case $K = \xi$ or η) can be expressed† in a simple form for *all values* of K, when a, b are subject to the condition

$$\mathrm{ab} \equiv 0 \pmod{K}; \quad [\text{Here } K = \xi, \eta, \text{ or } \xi\eta] \ldots\ldots\ldots\ldots (11).$$

The Table below shows the (± 1) value of $(K/p)_4$ as dependent on the forms of K, a, b.

[Herein K, a, α, β are all odd, and $\mathrm{b} = 2\omega$; (ω being odd)]......(12).

a	b	K	$(K/p)_4$	K	$(K/p)_4$	K	$(K/p)_4$	K	$(K/p)_4$
$K\alpha$,	.	$8k+1$,	$+1$	$8k+3$,	$+1$	$8k+5$,	-1	$8k+7$,	-1
. ,	$2K\beta$	$8k+1$,	$+1$	$8k+3$,	-1	$8k+5$,	$+1$	$8k+7$,	-1

When the condition (11) is fulfilled, it is hereby easy to deduce the (± 1) values of $(\xi/p)_4$, $(\eta/p)_4$; and then from them the (± 1) values of $(x/p)_4$, $(y/p)_4$ required for testing (9); or, if ξ, η be assumed, one can find the value of 2^κ in (10) required to satisfy (9).

The only advantage of this Rule, which is of course of very limited applicability, is that it is very easily tried.

Ex.

$p = 29 = 4.7 + 1 = 5^2 + 2^2$; $(5/p)_4 = -1$, $(4/p)_4 = -1$; $5^7 - 4^7 \equiv 0 \pmod{p}$

$p = 293 = 4.73 + 1 = 17^2 + 2^2$; $(17/p)_4 = +1$, $(16/p)_4 = +1$; $17^{73} - 16^{73} \equiv 0 \pmod{p}$

$p = 3413 = 4.853 + 1 = 7^2 + 58^2$; $(29/p)_4 = +1$, $(7/p)_4 = -1$, $(4/p)_4 = -1$; $29^{853} - 28^{853} \equiv 0 \pmod{p}$

---

* The author's Tables of "Quadratic Partitions," London, 1904, give these partitions for all primes up to $p \ngtr 100000$.

† *see* Père Th. Pépin's *Memoire sur les lois de réciprocité relatives aux résidus de puissances*, Rome, 1878, Art. 30-37; but, note that several misprints require correction.

8. *Divisors in general* (Complete Rule). Let a be any auxiliary base whose Haupt-Exponent $f = nq$, *i.e.* such that

$$a^f \equiv +1 \pmod{p = 2nq\varpi + 1}; \quad [f = nq \text{ is a minimum}; \ n \text{ may } = 1] \ldots (13).$$

And, let $x \equiv a^\xi$, $y \equiv a^\eta \pmod p$.

Then the Rule that $p = (2nq\varpi + 1)$ should be a divisor of N_q is

$$N_q \equiv 0 \pmod p, \text{ if } \xi \equiv \eta \pmod n \ldots\ldots\ldots\ldots (14).$$

For, taking the Residues of ξ, η to modulus n,

Let $\qquad \xi = \lambda n + \alpha, \quad \eta = \mu n + \beta.$

Then
$$\begin{aligned} x^q - y^q = a^{\xi q} - a^{\eta q} &= a^{\lambda nq + \alpha q} - a^{\mu nq + \beta q}, \\ &= a^{\lambda f} . a^{\alpha q} - a^{\mu f} . a^{\beta q}, \\ &\equiv a^{\alpha q} - a^{\beta q} \pmod p; \ [\text{for } a^f \equiv +1, \text{ mod } p]. \\ &\equiv 0 \pmod p, \text{ if } \alpha = \beta. \end{aligned}$$

But $\alpha = \beta$ gives $\xi - \eta \equiv 0 \pmod n$, which proves the Theorem.

When the auxiliary base (a) is a *primitive root* of p, then $f = p - 1$, and the Theorem necessarily holds.

The conditions (13, 14) here given are necessary and sufficient, and include all the preceding cases (Art. 6, 7). Their direct application unfortunately involves a great deal of labor in actual cases when suitable Tables are not available: in such cases it is advisable to choose the auxiliary base such that n shall be as small as possible—(preferably $n = 1$)—as this greatly facilitates the labor. It is proposed now to show how the above Rule can be easily applied with the help of suitable Tables.

9. *Use of the Canon Arithmeticus.* This well-known Canon* gives two Tables for every prime $p \not> 1000$, and also for every prime-power $p^\kappa \not> 1000$. The right-hand Table gives—in the body of the Table—the exponents (here denoted by ξ, η) to which the "base" (which is always a primitive root in this Table) must be raised to yield as Residues the numbers shown as the "Argument" of the Table (these are the x, y of this Paper).

To use this Table for the present purpose. Take

$n = (p-1) \div q$, when the modulus is a prime (p) ....(15a),

$n = p^{\kappa-1} . (p-1) \div q$, when the modulus is a prime-power (p^κ).....(15b).

Examine the *adjacent numbers* (*i.e.* ξ, η) in the body of the Table. Any pair (ξ, η) which have the *same Residue* $\alpha = \beta$,

* Jacobi's *Canon Arithmeticus*, Berlin, 1839.

when divided by n, (so that $\xi \equiv \eta$, mod n) will yield the required pairs of successive numbers (x, y) in the "Argument" of the Table. This search is easy to do: the only labor is that of dividing each pair of ξ, η by n. Thus, up to the limit of this Canon (p and $p^\kappa \not> 1000$), it is easy to find all the pairs of numbers (x, y) suited to a given exponent (q) for every prime (p) and prime-power (p^κ) as divisor.

9*a*. *Small divisor Table.* Tab. I. (at end of this Paper) gives, for every prime and prime-power (p and $p^\kappa \not> 1000$) of form $p = (2q\varpi + 1)$, the larger (x) of the two bases (x, y) giving

$$N_q = x^q - y^q \equiv 0 \text{ (mod } p \text{ or } p^\kappa),$$

for all *prime*-exponents $q > 3$, but $\not> 50$, up to a limit of x, marked X in the Table, viz.

$$X \not> p, \text{ or } \not> 50, \text{ when } q = 5; \quad X \not> 20, \text{ when } q > 5.$$

In a few cases the limit (X) is higher. This Table was computed from† the Canon Arithmeticus as above described.

10. *Use of Special Congruence-Tables.* The author has compiled‡ a Table of solutions of the Congruences

$$2^{x_0} \equiv \pm z^{\alpha_0} \text{ (mod } p \text{ and } p^\kappa), \; [z = 3, 5, 7, 11; \; p \text{ and } p^\kappa \not> 10^4] \ldots (16),$$

where α_0 = absolutely least exponent of z in above,

x_0 = least exponent of 2 going with z^{α_0}.

From this it is possible—by aid of the Haupt-Exponents§ (ξ_2, ξ_z) of 2 and z—to find congruences of form—

$$x^h \equiv +y^k \text{ (mod } p \text{ and } p^\kappa) \ldots\ldots (17),$$

connecting any pair (x, y) of the following pairs of bases—

$x = 3, 4, 5, 6, 7, 8, 9, 10, 11, 12; \; 15, 16; \; 21, 22;$ &c.

$y = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11; \; 14, 15; \; 20, 21;$ &c.

From (17) it follows that

$$x^{m\xi + h} \equiv +y^{m'\eta + k} \text{ (mod } p \text{ and } p^\kappa) \ldots\ldots (17a).$$

where ξ, η are the Haupt-Exponents of x, y.

---

† Unfortunately this Canon has many misprints, (a long list is given at the end of the volume). A list of the new errors discovered in course of preparing the present Table is given at end of this Paper.

‡ In conjunction with Mr. H. J. Woodall, A.R.C.Sc. This Table is in the press and will shortly be published.

§ The Haupt-Exponents (ξ_2, ξ_z) of 2 and z are the *least* exponents giving $2^{\xi_2} \equiv +1$ and $z^{\xi_z} \equiv +1$ (mod p and p^κ). The author has—in conjunction with Mr. H. J. Woodall—compiled a Table of the Haupt-Exponents (ξ) of each of the small bases 2, 3, 5, 6, 7, 10, 11, 12, for every prime and prime-power (p and $p^\kappa \not> 10^4$): this Table is in the press and will shortly be published.

Now, let m, m' be determined (if possible) so that

$$m\xi + h = m'\eta + k = q \text{ (a prime)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (18).$$

Then will $\quad N_q = x^q - y^q \equiv 0 \pmod{p \text{ or } p^\kappa}$ ....(18a),

so that hereby p or p^κ is a divisor of N_q.

10a. *Simple Case with Congruence Tables.* It is somewhat difficult to solve Eq. (18) in the general case. But, when the bases x, y are

$$x = 3,\ 4,\ 5,\ 8,\ 9 \text{ with } y = 2,\ 3,\ 4,\ 7,\ 8,$$

the above Congruence-Tables are *directly* available, and the process (detailed below) is comparatively easy.

The preliminary conditions are:—

1°. $p-1$, ξ_2, ξ_x must *each* contain q.

2°. $\xi_2 : \xi_z$ (or $\nu_z : \nu_2$) must = one of $2:1$, $1:1$, $1:2$.

3°. α_0 must $=1$, if $x = 3, 4, 5, 8$; α_0 must $=1$ or 2, if $x = 9$.

4°. If $2^{x_0} \equiv -z^{\alpha_0}$, ξ_2 must be *even* (except when $x = 9$).

When these conditions are fulfilled, the Table below shows, for the above values of the elements (x, y), the special condition required that p should be a divisor. This condition is of form

$$x_0 \text{ or } X_0 \equiv +1,\ 2,\ 3 \pmod{\xi_2/q}; \quad [X_0 = x_0 + \tfrac{1}{2}\xi_2] \ldots\ldots\ldots\ldots (19).$$

It requires certain relations as to ξ_2 being *odd* or *even*, depending on x_0 being odd or even, as shown in the Table (the two sets shown are *alternative*). The four conditions (1° to 4°) above, along with one of those marked "Preliminary" in the Table, rule out by far the greater number

Datum (mod p)	*Preliminary* x_0	ξ_2	x_0	ξ_2	*Condition* (19) (mod ξ_2/q)	*Result* (mod p)
$2^{x_0} \equiv +3$	ω,	.	ϵ,	ω	$x_0 \equiv +1$	$3^q - 2^q \equiv 0$
$+3$	ω,	ω	ϵ,	.	$+2$	$4^q - 3^q \equiv 0$
$+5$	ω,	ω	ϵ,	.	$+2$	$5^q - 4^q \equiv 0$
$+7$	ω,	.	ϵ,	ω	$+3$	$8^q - 7^q \equiv 0$
$2^{x_0} \equiv -3$	ω,	$4i$	ϵ,	2ω	$X_0 \equiv +1$	$3^q - 2^q \equiv 0$
-3	ω,	2ω	ϵ,	$4i$	$+2$	$4^q - 3^q \equiv 0$
-5	ω,	2ω	ϵ,	$4i$	$+2$	$5^q - 4^q \equiv 0$
-7	ω,	$4i$	ϵ,	2ω	$+3$	$8^q - 7^q \equiv 0$
$2^{x_0} \equiv \pm 3$	.	ω	.	.	$2x_0 \equiv +3$	$9^q - 8^q \equiv 0$
$2^{x_0} \equiv +3^2$	ω,	.	ϵ,	ω	$x_0 \equiv +3$	$9^q - 8^q \equiv 0$
$2^{x_0} \equiv -3^2$	ω,	ϵ	.	.	$X_0 \equiv +3$	$9^q - 8^q \equiv 0$

of primes as possible divisors, leaving very few to be tried by this final Test (19): this Test, when satisfied, involves Result (18*a*).

11. *Use of Haupt-Exponent Tables.* From the Haupt-Exponent Table, described in the footnote § to Art. 10, as giving the Haupt-Exponents (ξ) of *all* the small bases x or $y = 2, 3, 5, 6, 7, 10, 11, 12$ for all primes and prime-powers p and $p^\kappa \ngtr 10000$, it is easy to pick out the pairs of bases x, y up to $x \ngtr 12$, which have the *same* Haupt-Exponent (ξ), giving—

$$x^\xi - y^\xi \equiv 0 \pmod{p \text{ or } p^\kappa} \quad\ldots\ldots(20).$$

If now $\xi = nq$; then, since $x^q - y^q$ is thereby one of the factors of $(x^\xi - y^\xi)$, it is *possible* that

$$N_q = x^q - y^q \; \textit{may} \equiv 0 \pmod{p \text{ or } p^\kappa},$$

but, to be certain of this would require special testing which might involve considerable labor. Two cases are, however, obvious *at sight*, viz.:

$$\text{If } \xi = q \text{ or } = 2q; \text{ then } N_q = x^q - y^q \equiv 0 \pmod{p \text{ or } p^\kappa} \quad\ldots\ldots(20a),$$

The only advantage of the use of this Table is that the Results (20*a*) are obtained *at sight*: they are of little use for *practical factorisation*, as the divisors > 1000 so obtained from (20*a*) all belong to high* exponents (q).

12. *Square, Cube, &c., Divisors.* In marked contrast to Mersenne's Numbers, for which no square divisors have as yet† been discovered, the Quasi-Mersennians have square, cube, &c., divisors in particular orders (q) for certain bases (x, y); but, it appears not to be known whether square divisors are impossible for certain bases (x, y).

When $p^\kappa \ngtr 1000$, the elements (x, y) of the N_q which have p^κ as a divisor can be found by the process of Art. 9 from the *Canon Arithmeticus.* And, when $p^\kappa \ngtr 10000$, the elements (x, y)—named in Art. 10—of the N_q which have p^κ as a divisor can be found by the processes of Art. 10, 10*a* from the Special Congruence-Tables therein named.

---

* Only one case of $\xi = q < 50$; viz. $p = 1231$ has $\xi = q = 41$ for the bases $x, y = 11, 10$.

† It is stated definitely by Mr. F. Proth in *Comptes Rendus des Séances de l'Acad. des Sciences*, Paris, T. 83, p. 1288, that $2^p - 2 \not\equiv 0 \pmod{p^2}$; but no proof is quoted, no statement made of existence of any proof: so that at present it can only be accepted as *probably true*. To test this question the author has tried *all prime divisors* p up to $p \ngtr 1000$, and finds that $2^p - 2 \not\equiv 0 \pmod{p^2}$ up to that limit.

13. *Factorisation-Tables.* Two Tables of factorisation of $N_q = x^q - y^q$ $[x - y = 1]$ are given at end of this Paper—

Tab. III. (Small powers q). $q = 5, 7, 11, 13$.

Tab. IV. (Small bases x, y). $x = 3$ to 12, $y = x - 1 = 2$ to 11; $q = 17$* to 47.

In these Tables all small prime divisors $\not> 1000$ have been cast out by aid of Tab. I., and many of those $> 10^3$ but $\not> 10^4$ have been cast out by aid of the Tables described in Art. 10, 10*a*.

13*a*. *Cuban Primes* (Tab. II.). For the case of the Cubans $N_3 = (x^3 - y^3)$, no Factorisation Table is given, as these numbers can be resolved by the large Factor-Tables alone up to $x = 1827$ (see Art. 2). It has been thought better to give a complete List (Tab. II.) of the *primes* of this form, up to 1 million.

This gives

$$\left.\begin{aligned} N_3 &= (3x^2 - 3x + 1) = (3y^2 + 3y + 1) \ldots\ldots \\ &= (y + \tfrac{1}{2}x)^2 + 3(\tfrac{1}{2}x)^2, \text{ when } x = \epsilon \ldots\ldots \\ &= (x + \tfrac{1}{2}y)^2 + 3(\tfrac{1}{2}y)^2, \text{ when } y = \epsilon \ldots\ldots \end{aligned}\right\} \ldots(21).$$

$$\text{Hence}\quad \left.\begin{aligned} &(2/p)_3 = 1, \text{ when } x \text{ or } y = 6i \ldots\ldots \\ &(2/p,\ 3/p,\ 6/p,\ \&\ 12/p)_3 = 1, \text{ when } x \text{ or } y = 18i \ldots\ldots \\ &(3/p)_3 = 1, (2/p,\ 6/p,\ \&\ 12/p) \neq 1, \text{ when } x = \epsilon\ \&\ y(x+y) = 9\omega \\ &(3/p)_3 = 1, (2/p,\ 6/p,\ \&\ 12/p) \neq 1, \text{ when } y = \epsilon\ \&\ x(x+y) = 9\omega \end{aligned}\right\} \ldots(21a).$$

14. *Algebraic Factorisation.* These numbers (N_q) differ markedly from Mersenne's Numbers in one respect, viz. that they can—in certain cases—be *algebraically* resolved into two co-factors, say *L. M.* These cases are of *three kinds*, named below, and are treated of in the Articles quoted.

i. *Perfect Squares*, Art. 15. ii. *Dimorphs*, Art. 16—20*b*.

iii. *Aurifeuillians*, Art. 21—23*d*.

Notation. In the arithmetical examples given of the Classes ii., iii., the two co-factors (L, M) will—for the sake of distinction—be separated by a colon (:); the smaller factor will usually be denoted by L, and the larger by M.

15. *Perfect Squares* $(q = 3)$. The only case known (to the author) in which $N_q = (x^q - y^q)$ can be a perfect square $= z^2$, is when $q = 3$.

And, in this case, since

$$N_3 = x^3 - y^3 = \frac{x^3 - y^3}{x - y} = z^2, \text{ is of form } (A^2 + 3B^2) \ldots\ldots(22),$$

it follows that

$$z = \alpha^2 + 3\beta^2, \quad N_3 = z^2 = (\alpha^2 - 3\beta^2)^2 + 3(2\alpha\beta)^2 = A^2 + 3B^2 \ldots\ldots(23),$$

whence $$A = \alpha^2 - 3\beta^2, \quad B = 2\alpha\beta \ldots\ldots(23a).$$

---

* The factorisation of N_q, with $q < 17$, is given for the small bases in Tab. III.

Also $x-y=1$ requires x or y *even*, and y or x *odd*. The two cases (x or y *even*) must be treated separately.

Case i. $x=\epsilon$; $N=(\frac{1}{2}x+y)^2+3(\frac{1}{2}x)^2$	Case ii. $y=\epsilon$; $N=(x+\frac{1}{2}y)^2+3(\frac{1}{2}y)^2$
*$\frac{1}{2}x+y=3\beta^2-\alpha^2$, $\frac{1}{2}x=2\alpha\beta$	*$x+\frac{1}{2}y=\alpha^2-3\beta^2$, $\frac{1}{2}y=2\alpha\beta$ ...(24a),
$x=4\alpha\beta$, $y=3\beta^2-\alpha^2-2\alpha\beta$	$x=\alpha^2-2\alpha\beta-3\beta^2$, $y=4\alpha\beta$ ...(24b),
$x-y=(\alpha+3\beta)^2-3(2\beta)^2=+1$	$x-y=(\alpha-3\beta)^2-3(2\beta)^2=+1$.(24$c$).

Hence $x-y$ is—(in both Cases)—of form $x-y=\tau^2-3\upsilon^2\equiv+1$ (with υ *even*); and every solution (τ, υ) of this Pellian (in which υ is *even*) leads to two square forms of N_q (one under each of above Cases), viz.

Under Case i., when $\beta>\alpha$	Under Case ii., when $\alpha>\beta$.
$\alpha=\tau-\frac{3}{2}\upsilon$, $\beta=\frac{1}{2}\upsilon$	$\alpha=\tau+\frac{3}{2}\upsilon$, $\beta=\frac{1}{2}\upsilon$ ....(25).

Ex. The Table below shows the successive solutions (τ, υ) of the Pellian (in which υ is *even*), and the consequent values of the "2^{ic} parts" (α, β) of z; also the elements (x, y) of N, and the value of z itself.

i. $x=\epsilon$, $\beta>\alpha$	$r=$	1	3	5	7
	τ, υ	7, 4	97, 56	1351, 780	18817, 10864
	α, β	1, 2	13, 28	181, 390	2521, 5432
	x, y	8, 7;	1456, 1455;	282360, 282359;	54776288, 54776287;
	z	13	2521	489061	94875313
ii. $y=\epsilon$, $\beta<\alpha$	$r=$	2	4	6	8
	τ, υ	7, 4	97. 56	1351, 780	18817, 10864
	α, β	13, 2	181, 28	2521, 390	35113, 5432
	x, y	105, 104;	20273, 20272;	3932761, 3932760;	762935265, 762935264;
	z	181	35113	6811741	1321442641

Note that, if the successive solutions of $\tau^2-3\upsilon^2=+1$ be marked with the suffixes $r=0, 1, 2, 3,$ &c.; and if the successive values of (α, β), (x, y), z be marked with the suffixes (r),

$r=1, 3, 5, \ldots$, in Case i.; $r=2, 4, 6, \ldots$, in Case ii.

then $\alpha_{2r+1}=\alpha_{2r}$, $\beta_{2r-1}=\beta_{2r}=\frac{1}{2}\upsilon_{2r}$ ....(26).

16. *Dimorphs.* These are of two kinds, which will be found treated of in the Articles quoted.

Reduced Binomials, Art. 17 to 18b. $N_q=\dfrac{x^q-y^q}{x-y}=\dfrac{x'^q-y'^q}{x'-y'}$, [$x-y=1$; y' may be $-$]..(26a).

Simple Binomials, Art. 19 to 20b. $N_q=x^q-y^q=x'^q-y'^q$, [$x-y=1$; y' may be $-$]..(26b).

It is easy to see that *pure* Dimorphs of either kind, *i.e.* with $x-y=1=x'-y'$, are *impossible* in the same order

* The cases of $\frac{1}{2}x+y=\alpha^2-3\beta^2$ in Case i., and of $x+\frac{1}{2}y=3\beta^2-\alpha^2$ in Case ii, are omitted as they lead only to results of form $x-y=3\upsilon^2-\tau^2=+1$, which is impossible.

$(q=q')$, because N_q increases with increase of x: this involves in both cases—

$$x'-y' > x-y, \text{ and } >1 \qquad \text{(26c)}.$$

The former are taken first, as being the easier of treatment. In both kinds the Dimorphism provides the data for *algebraic* resolution into a pair of co-factors (L, M).

17. *Reduced Binomial Dimorphs.* These are of form—

$$N_q = \frac{x^q-y^q}{x-y} = \frac{x'^q-y'^q}{x'-y'},\ [x-y=1,\ y' \text{ may be } -] \qquad (27).$$

Now each of these forms may be expressed in its own quadratic partition, of the same form for each, viz.

$$N_q = t^2-qu^2 = t'^2-qu'^2, \text{ when } q=4k+1 \qquad (27a),$$
$$N_q = t^2+qu^2 = t'^2+qu'^2, \text{ when } q=4k-1 \qquad (27b),$$

and these two partitions will in each case be *different*, *i.e.* not algebraically inter-convertible. The number N_q can therefore be resolved into two co-factors (L, M) by known rules.

17a. *Case of* $q>5$. No examples are known (to the author) of such Dimorphs, when $q>5$. It appears in fact not to be known whether this sort of Dimorphism is possible when $q>5$.

17b. *Quintans* $(q=5)$. Very few Dimorph Quintans are known to the author, and only two for the present case $(x-y=1)$, viz.—

$$(4^5-3^5)\div(4-3)=(5^5-1^5)\div(5-1)=11:71;$$
$$(5^5-4^5)\div(5-4)=(7^5+1^5)\div(7+1)=11:191;$$

These suffice to prove the existence of this Dimorphism when $q=5$; but no general rule has been found for their formation.

18. *Cuban Dimorphs.* It will now be shown, first how to form Cuban* Dimorphs, *i.e.*

$$N_3=N'_3;\ \text{where } N_3=(x^3-y^3)\div(x-y),\ N_3'=(x'^3-y'^3)\div(x'-y') \qquad (28),$$

in a perfectly general manner and then (Art. 18b) how to factorise large numbers $(N_3>10^7)$ of this kind.

But, note that every Cuban is expressible in three Cuban forms,

$$N_3=\frac{x^3-y^3}{x-y}=\frac{(x+y)^3+x^3}{(x+y)+x}=\frac{(x+y)^3+y^3}{(x+y)+y};\ [x,\ y \text{ both } +] \qquad (29),$$

* Note the terminology: here $(x^3\mp y^3)\div(x\mp y)$ is termed a *Cuban*, whilst $(x^3\mp y^3)$ is a *Cubic* (compare Art. 20).

These, being algebraically inter-convertible, are *equivalent forms*, and are therefore *not reckoned different* forms. To be of any use in factorisation, it is essential that the two forms N, N' should be *different* (*i.e.* non-equivalent) forms: the term *Dimorph* is accordingly here used to imply (arithmetical) *equality* with (algebraic) *non-equivalence.*

Write $\quad x-y=\lambda,\ \ x'-y'=\lambda',\ \ [\lambda'\neq\lambda]$.........(30).

Eliminating x, x', the Dimorph Equation (28) becomes

$$y^2+y\lambda+\tfrac{1}{3}\lambda^2=y'^2+y'\lambda'+\tfrac{1}{3}\lambda'^2.$$

Write now $\quad 2y+\lambda=l,\ \ 2y'+\lambda'=l'$...............(31).

whereby the Dimorph Equation reduces to

$$l^2-l'^2=\tfrac{1}{3}(\lambda'^2-\lambda^2). \qquad \text{(32).}$$

The last equation (32) may be conveniently used for generating Dimorphs by assigning any (unequal) integer values—(not multiples of 3)—to λ, λ', and factorising the dexter quantity $\frac{1}{3}(\lambda'^2-\lambda^2)$ in every possible way into two co-factors, say P, Q, so that

$$l^2-l'^2=\tfrac{1}{3}(\lambda'^2-\lambda^2)=P_0Q_0=P_1Q_1=P_2Q_2=\ldots \qquad \text{(33).}$$

Every way in which this can be done gives values of l, l',

$$l+l'=P,\ \ l-l'=Q;\ \ \ l=\tfrac{1}{2}(P+Q),\ \ l'=\tfrac{1}{2}(P-Q) \qquad \text{(34).}$$

The values of x, y, x', y' corresponding, are given from (30) by

$$x=\tfrac{1}{2}(l+\lambda),\ \ y=\tfrac{1}{2}(l-\lambda);\ \ \ x'=\tfrac{1}{2}(l'+\lambda'),\ \ y'=\tfrac{1}{2}(l'-\lambda') \qquad \text{(35).}$$

It will be found that all possible cases can be formed by taking λ, λ' either *both odd*, or *one odd and one even*: but the latter pair of values will be found more convenient.

The quantity $\frac{1}{3}(\lambda'^2-\lambda^2)$ has always one *algebraic* factorisation, viz. *one* of the following:—[Here P is supposed $> Q$].

1°. $P=\lambda'-\lambda,\quad Q=\frac{1}{3}(\lambda'+\lambda)$; which gives $x'=x+y,\ y'=-x$....(36*a*),

2°. $P=\frac{1}{3}(\lambda'+\lambda),\ Q=(\lambda'-\lambda)$; which gives $x'=x+y,\ y'=-x$....(36*b*),

3°. $P=\lambda'+\lambda,\quad Q=\frac{1}{3}(\lambda'-\lambda)$; which gives $x'=x+y,\ y'=-y$....(36*c*),

These values of x', y' give N' in one of the *equivalent forms* (29) of N, whereas N' is required in a form *different* to that of N: so these values of P, Q do not yield Dimorphs. All other factorisations P, Q of $\frac{1}{3}(\lambda'^2-\lambda^2)$—(if there be any others)—yield *different forms* of N, N', *i.e.* yield Dimorphs.

When $\lambda'-\lambda=3$, and $(\lambda'+\lambda)$ is a prime, then $Q=1$, $P=(\lambda'+\lambda)$ are the *only pair* of co-factors (this is Case 3° above); and in this Case there are *no Dimorphs.* But all

other values of λ, λ' give this pair of co-factors $Q=1$, $P=\frac{1}{3}(\lambda'^2-\lambda^2)$ different from any of the above three Cases, and therefore yielding one Dimorph.

Considering all pairs of co-factors (P, Q), the maxima of x, y, x', y', N arise when $(P-Q)$ is a maximum, *i.e.* when $Q=1$, $P=\frac{1}{3}(\lambda'^2-\lambda^2)$: the values of x, y, x', y', N decrease steadily as $(P-Q)$ decreases: y remains $+$, y' changes sign from $+$ to $-$ when nearing the critical case 1°, 2°, or 3° above; and finally the minima of x, y, x', y', N occur with $(P-Q)$ a minimum.

18*a*. *Case of Quasi-Mersennians.* For this case $\lambda=x-y=1$, leaving $\lambda'=x'-y'$ the only arbitrary parameter.

Ex. In order to show the power of this process in yielding large factorisable numbers ($N_3=x^3-y^3$), together with the data for their factorisation (provided by the Dimorphism)—

Take $\lambda'=1000$, which gives $PQ=\frac{1}{3}(\lambda'^2<\lambda^2)=333333=1.3^2.7.11.13.37$;

This can be resolved into two co-factors (P, Q) in 23 ways; the lesser factor (Q) being

$Q=1, 3, 7, 9, 11, 13, 21, 33, 37, 39, 63, 77, 91, 99,$
$111, 117, 231, 259, 273, 333, 407, 429, 481$;

The Table below gives the values of $P, Q, l, l', x, y, x', y'$ for a few selected cases including

1°. The maximum of N, given by $Q=1$.

2°. The cases just before and after the change of sign of y' from $+$ to $-$.

3°. The algebraic case, given by $Q=\frac{1}{3}(\lambda'-\lambda)=333$ (not giving a Dimorph).

4°. The minimum of N, given by $P-Q=$minimum.

The right-hand column—(headed "Fig")—shows the number of figures in N.

P	Q	l	l'	x	y	x'	y'	Fig.
333333,	1	166667,	166666	83334,	83333	83833,	82833	11
111111,	3	55557,	55554	27779,	27778	28277,	27277	10
2849,	117	1483,	1366	742,	741	1183,	183	7
1443,	231	837,	606	419,	419	803,	-197	6
1001,	333	667,	334	334,	333	667,	-333	6
693,	481	587,	106	294,	293	553,	-447	6

18*b*. *Factorisation of Cuban Dimorphs.* Every Cuban

$$N=(x^3-y^3)\div(x-y)=x^2+xy+y^2 \quad\ldots\ldots\ldots\ldots(37),$$

is algebraically expressible in the 2^{ic} form $N=A^2+3B^2$ by the formulæ

$$N=(\tfrac{1}{2}x-y)^2+3(\tfrac{1}{2}x)^2, \qquad \text{if } x=\epsilon\ldots\ldots\ldots\ldots(37a),$$

$$=(x-\tfrac{1}{2}y)^2+3(\tfrac{1}{2}y)^2, \qquad \text{if } y=\epsilon\ldots\ldots\ldots\ldots(37b),$$

$$=\{\tfrac{1}{2}(x-y)\}^2+3\{\tfrac{1}{2}(x+y)\}^2, \text{ if } xy=\omega\ldots\ldots\ldots\ldots(37c).$$

If the elements (x, y, x', y') of a Cuban Dimorph

$N = N'$; where $N = (x^3 - y^3) \div (x - y)$, $N' = (x'^3 - y'^3) \div (x' - y')$,

be *given*: and factorisation of N be required, the first step is to express N, N' in the 2^{ic} form

$$N = A^2 + 3B^2, \quad N' = A'^2 + 3B'^2 \quad \text{.........................(38)},$$

by the above formulæ $(37a, b, c)$. These two forms must be *different*, because the Cuban forms from which they rise are *different* (being Dimorph), and N must therefore be *composite*. Two methods of factorisation are available.

METHOD i.

Here $$N = \frac{(AB')^2 - (A'B)^2}{B'^2 - B^2}, \quad \text{or} \quad = \frac{(AB')^2 - (A'B)^2}{\frac{1}{3}(A^2 - A'^2)} = N'.$$

Hence,

$$L \text{ or } M = \frac{AB' - A'B}{(B' - B) \text{ or } (B' + B)}, \quad M \text{ or } L = \frac{AB' + A'B}{(B' + B) \text{ or } (B' - B)} \text{...(39)}.$$

[This Method has the double disadvantage of requiring the formation of the products AB', $A'B$ (numbers nearly as large as N), and of finding the common factors of the numerator and denominator, both of which are tedious matters when N is large. The Method below has the great advantage of dealing with smaller numbers throughout.]

METHOD ii. Let L, M be the co-factors of $N = N'$. Then L, M are necessarily of form

$$L = \eta_1^2 + 3\theta_1^2, \quad M = \eta_2^2 + 3\theta_2^2; \quad \text{and } N = L.M \text{...............(40)}.$$

Hence, by known Rules, the ratios of $\eta_1 : \theta_1$, $\eta_2 : \theta_2$ are given by

$$\frac{\eta_1}{\theta_1} = \frac{A' + A}{B - B'} = 3\frac{B + B'}{A' - A}, \quad \frac{\eta_2}{\theta_1} = \frac{A' + A}{B + B'} = 3\frac{B - B'}{A' - A} \text{.................(41)},$$

and, since the "2^{ic} parts" (η_1, θ_1), (η_2, θ_2) of each partition should be mutually prime, it follows that, when the above fractions have been *reduced to their lowest terms*, then

The reduced numerators give η_1, η_2......................(41*a*).

The reduced denominators give θ_1, θ_2... ....(41*b*).

Ex. The highest of the Dimorph Cubans in Ex. of Art. 18*a* is a good example of the easiness of this process (Method ii.), even with high numbers. (Here $N = N' = 20833416667$).

$$N = 83334^3 - 83333^3 = (83833^3 - 82833^3) \div (83833 - 82833) = N'.$$

The formulæ $(37a, c)$ give at once

$$N = 125000^2 + 3.41667^2 = 500^2 + 3.83333^2 = N';$$

And, the formulæ $(41, 41a, b)$ give

$$\frac{\eta_1}{\theta_1} = \frac{125500}{41666} = \frac{250}{83}, \quad \frac{\eta_2}{\theta_2} = \frac{125500}{125000} = \frac{251}{250},$$

whence, at once,

$$L = 250^2 + 3.83^2 = 83167 = 7.109.109; \quad M = 251^2 + 3.250^2 = 250501;$$

19. *Simple Binomial Dimorphs.* These are of forms

$$N = N'; \text{ where } N = x^q - y^q, \quad N' = x'^q - y'^q \text{ ....(42).}$$

No case is known (to the author) of such Dimorphism when $q > 3$; nor does it appear to be known whether this property is possible, or not, in that case.

20. *Simple Cubic* Dimorphs.* It will be shown, first how to form these Dimorphs in a general manner, and then (Art. 20*b*) how to factorise large numbers ($N > 10^7$) of this kind.

Let $\quad N = N', \text{ where } N = x^3 - y^3, \quad N' = x'^3 - y'^3$ ....(43).

Now write $\quad x - y = K\lambda, \quad x' - y' = K.\lambda'$ ....(44),

where K is the G.C.M. of $(x-y)$, $(x'-y')$,

so that $\quad \lambda, \lambda'$ are *mutually prime* ....(44*a*).

Also write $\quad Z = (x^3 - y^3) \div (x - y), \quad Z' = (x'^3 - y'^3) \div x' - y')$............(45),

so that $\quad N = K\lambda Z, \quad N' = K\lambda' Z'$ ....(45*a*),

Hence, it is clear that—(as $\lambda \neq \lambda'$)—N must contain λ', and N' must contain λ, so that

$$N \div K\lambda = Z, \quad N' \div K\lambda' = Z' \text{ ....(46).}$$

Hence λ, λ' must be of the forms

$$\lambda = \alpha^2 + 3\beta^2, \quad \lambda' = \alpha'^2 + 3\beta'^2; \quad [\lambda \neq \lambda'] \text{ ....(47).}$$

And, any factor of either N or N', which is not of form $(\alpha^2 + 3\beta^2)$, cannot be contained in either Z or Z', so must be contained in K, and is therefore a factor of both N, N'.

[In the case of Quasi-Mersennians $K = 1$, $\lambda = 1$, $\lambda' \neq \lambda$].

Writing now,

$$2x = 2l + K\lambda, \; 2y = 2l - K\lambda; \quad 2x' = 2l' + K\lambda', \; 2y' = 2l' - K\lambda' \text{......(48),}$$

the Dimorph equation reduces to

$$\lambda(2l)^2 - \lambda'(2l')^2 = \tfrac{1}{3}K^2(\lambda'^3 - \lambda^3) \text{ ....(49).}$$

[A certain similarity between the above procedure, and that previously used for the formation of Cuban Dimorphs (Art. 18) will be noticed; but the present case is much more difficult.]

This last equation may be used for generating Simple Cubic Dimorphs *directly*, by assigning any numerical values to K, λ, λ' (but λ, λ' are subject to (44*a*)). The equation then becomes an ordinary 2^ic Diophantine, wherein l, l' are the indeterminates. This equation—if solvable at all—is known to have an *infinite number* of solutions (l_r, l'_r), which can

---

* Note the terminology: here $(x^3 \mp y^3)$ is termed a *Cubic*; whilst $(x^3 \mp y^3) \div (x \mp y)$ is termed a *Cuban* (compare Art. 18).

be generated from any one (known) solution say (l_0, l'_0) by aid of the *unit-form* (whose solutions τ, v are supposed *known*,

$$\tau^2 - \lambda\lambda' v^2 = +1 \quad\text{......................}(50).$$

The obtaining of the first—or what may be called the *Basic*—solution of the Diophantine (for given values of K, λ, λ') is often very difficult. The following indirect process supplies *solvable cases* together with their *basic solution* more readily.

Small values of x, y, x', y' giving $N = N'$ can be found by searching a small Factorisation-Table of $N = x^3 - y^3$. Let these be x_0, y_0, x'_0, y'_0. The values of K, λ_0, λ'_0, are then given by the formulæ (44, 44*a*) and those of l_0, l_0' by

$$2x - K\lambda = 2l = 2y + K\lambda, \quad 2x' - K\lambda' = 2l' = 2y' + K\lambda' \text{...}(51).$$

These values of l_0, l_0' are the *basic solutions* of the Diophantine. From this solution an indefinite series of solutions (l_1, l_1'), (l_2, l_2'), &c., may be found by repeated applications of the unit-form in the usual process of solving such Diophantines. Each such solution (l, l') yields a set of the elements (x, y, x', y') by the formulæ (48):

20*a*. *Case of Quasi-Mersennians.* In this case

$$K = 1, \quad \lambda = 1, \quad \lambda' = x' - y' > 1 \quad\text{...............}(52),$$

and the Diophantine equation (49) simplifies to

$$l^2 - \lambda' . l'^2 = \tfrac{1}{3}(\lambda'^3 - 1) \quad\text{....................}(53).$$

When the *basic solution* (l_0, l'_0) is obtained—as above suggested—from a factorisation of small numbers $N = (x^3 - y^3)$, this gives in the first instance the basic values x_0, y_0, x'_0, y'_0: from which the *basic solution* (l_0, l'_0) of (53) is given at once by

$$2x_0 - 1 = 2l_0 = 2y_0 + 1, \quad 2x'_0 - \lambda' = 2l'_0 = 2y'_0 + \lambda' \text{......}(54).$$

The application of the *unit-form* $(\tau^2 - \lambda' v^2 = +1)$ then gives *two* new solutions $(2l_1, 2l_1')$ by the formulæ

$$l_1 = \tau l_0 \mp \lambda' v l'_0, \quad l'_1 = v l_0 \mp \tau l'_0, \ [\text{both signs} -, \text{ or both} +]\text{...}(55).$$

Each of these gives rise—by repeated application of the unit-form (with the + sign throughout)—to an infinite train of solutions: each of these solutions $(2l_r, 2l_r')$ gives rise to a corresponding Cubic Dimorph by the formulæ

$$2x_r = 2l_r + 1, \ 2y_r = 2l_r - 1; \ \ 2x'_r = 2l'_r + \lambda', \ 2y'_r = 2l'_r - \lambda' \text{...}(56),$$

[This Problem differs greatly from the preceding (Art. 18, 18*a*), in which the number of Cuban Dimorphs arising from a given $x' - y' = \lambda'$ is strictly

limited; whereas in the present case a given $x'-y'=\lambda'$ gives rise to a doubly infinite series of Cubic Dimorphs.]

Ex. The following Table shows the elements (x_0, y_0, x'_0, y'_0) of a number of small Cubic Dimorphs $(N_0=N_0')$, found as above explained (from a Factorisation Table), with the values of $\lambda=(x_0-y_0)=1$, $\lambda'=(x_0'-y_0')$, and of the quantity $\frac{1}{3}(\lambda'^3-\lambda^3)$ thence found: also the *basic solution* $(2l_0, 2l'_0)$ found from (53), and the *two* first-derived solutions $(2l_1, 2l_1')$ found from (55), and the elements (x_1, y_1, x'_1, y'_1) of the new Dimorphs arising from them found from (56).

x_0 y_0	x'_0 y'_0	λ λ'	$\frac{1}{3}(\lambda'^3-\lambda^3)$	$2l_0$ $2l'_0$	$2l_1$ $2l'_1$	x_1 y_1	x'_1 y'_1
6, 5	4, $\bar{3}$	1, 7	114	11, 1	67, 25	34, 33	16, 9
					109, 41	55, 54	24, 17
9, 8	6, $\bar{1}$	1, 7	114	17, 5	31, 11	16, 15	9, 2
					241, 91	121, 120	49, 42
19, 18	10, $\bar{3}$	1, 13	732	37, 7	7633, 2117	3817, 3816	1065, 1052
					40393, 11203	20197, 20196	5608, 5595
41, 40	17, $\bar{2}$	1, 19	2286	81, 15	2655, 609	1328, 1327	314, 295
					24885, 5709	12443, 12442	2864, 2845
54, 53	19, $\overline{12}$	1, 31	9930	107, 7	103399, 18571	51700, 51699	9301, 9270
					221881, 39851	110941, 110940	19941, 19910
71, 70	23, $\overline{14}$	1, 37	16884	141, 9	6297, 1035	3149, 3148	536, 499
					14289, 2349	7145, 7144	1193, 1156
115, 114	34, $\bar{3}$	1, 37	16884	229, 31	2953, 485	1477, 1476	261, 224
					30481, 5011	15241, 15240	2524, 2487

The above process will now be further illustrated by the following Table showing the generation of the successive Cubic Dimorphs from the successive solutions $(2l_r, 2l'_r)$ of the Diophantine. The example here taken is No. 1° of the Table preceding—

$$x_0^3-y_0^3=6^3-5^3=4^3-(\bar{3})^3=x'^3_0-y'^3_0; \quad \text{giving } \lambda=1,\ \lambda'=7.$$

These give the Diophantine $(2l)^2-7(2l')^2=+114$,

whose basic solution is $2l_0=11$, $2l'_0=1$.

The double series of successive solutions $(2l_r, 2l'_r)$ are shown in the Table below as far as the fourth step $(r=4)$: followed by the elements (x_r, y_r, x'_r, y'_r) the successive Cubic Dimorphs arising therefrom. The co-factors (L, M) of these Cubics, found by a process to be presently explained (Art. 20*b*), are shown in the right-hand column: the factors λ, λ' are of course common to all the Cubics of these series.

The right-hand column (headed "Figs") shows the number of figures in each of the final numbers N: these numbers well illustrate the power of the process in producing high factorisable numbers together with the data for their factorisation.

r	$2l_r$ $2l'_r$	x y	x' y'	λ, λ' L M	Figs
0	11, 1	6, 5	4, −3	1, 7; 1 : 13;	2
1	67, 25	34, 33	16, 9	1, 7; 13 : 37;	4
2	1061, 401	531, 530	204, 197	1, 7; 103 : 1171;	7
3	16909, 6391	8455, 8454	3199, 3192	1, 7; 49·67 : 43·731;	10
4	269483, 101855	134742, 134741	50931, 50924	1, 7; 26161 : 297421;	12
1	109, 41	55, 54	24, 17	1, 7; 19 : 67;	4
2	1733, 655	867, 866	331, 324	1, 7; 151 : 2131;	8
3	27619, 10439	13810, 13809	5223, 5216	1, 7; 4813 : 16981;	10
4	440171, 166369	220086, 220085	83188, 83181	1, 7; 7·5479 : 7·77323;	12

20*b*. *Factorisation of Simple Cubic Dimorphs.* Taking the general case, as before (Art. 18*b*)

$$N = x^3 - y^3 = x'^3 - y'^3 = N' \quad\ldots\ldots\ldots(57),$$

and, with the notation of Art. 20

$$x - y = K\lambda,\ x' - y' = K\lambda';\ Z = (x^3 - y^3) \div (x - y),\ Z' = (x'^3 - y'^3) \div (x' - y') \ldots(58).$$

Here the factor K, which would be found as the G.C.M. of $(x - y)$, $(x' - y')$, is to be cancelled from each of N, N'. Next λ, λ', Z, Z' are to be expressed in the 2^{ic} forms (see Art. 18)

$$\lambda = \alpha^2 + 3\beta^2,\ \ \lambda' = \alpha'^2 + 3\beta'^2,\ \ Z = \mathrm{a}^2 + 3\mathrm{b}^2,\ \ Z' = \mathrm{a}'^2 + 3\mathrm{b}'^2 \ldots\ldots\ldots(59),$$

whereby $N = N'$ reduces to

$$\frac{Z}{\lambda'} = \frac{\mathrm{a}^2 + 3\mathrm{b}^2}{\alpha'^2 + 3\beta'^2} = \frac{\mathrm{a}'^2 + 3\mathrm{b}'^2}{\alpha^2 + 3\beta^2} = \frac{Z'}{\lambda} \ldots\ldots\ldots(60).$$

These fractions are now to be reduced by the method of *conformal division** to the form

$$Z/\lambda' = A^2 + 3B^2 = A'^2 + 3B'^2 = Z'/\lambda \ldots\ldots\ldots(61).$$

These two 2^{ic} forms must necessarily be *different*—(because $N = N'$ is a Dimorph)—so that the quantity $Z \div \lambda'$ must be composite. Let the co-factors be L, M; these must necessarily be of the form

$$L = \eta_1^2 + 3\theta_1^2,\ \ M = \eta_2^2 + 3\theta_2^2 \ldots\ldots\ldots(62).$$

Then—as in Art. 18*b*—the ratios of $\eta_1 : \theta_1$, $\eta_2 : \theta_2$ are given by the formulæ—

$$\frac{\eta_1}{\theta_1} = \frac{A' + A}{B - B'} = 3\frac{B + B}{A' - A'},\quad \frac{\eta_2}{\theta_2} = \frac{A' + A}{B + B'} = 3\frac{B - B'}{A' - A} \ldots\ldots\ldots(63),$$

and, when these fractions have been *reduced to the lowest terms*, the "2^{ic} parts" are given thus—

The reduced numerators give η_1, η_2 ....(63*a*),

The reduced denominators give θ_1, θ_2 ....(63*b*).

Ex. The example in the last line of the second Table of Art. 20*a* gives a good example of the comparative easiness of this process in resolving high numbers—

$$N = 220086^3 - 220085^3 = 83188^3 - 83181^3 = N',$$

Here $x - y = K\lambda = 1$, $x' - y' = K\lambda' = 7$; whence $K = 1$, $\lambda = 1$, $\lambda' = 7 = 2^2 + 3.1^2$,

$$Z = (y + \tfrac{1}{2}x)^2 + 3(\tfrac{1}{2}x)^2,\quad Z' = (y' + \tfrac{1}{2}x')^2 + 3(\tfrac{1}{2}x')^2,$$

$$\frac{Z}{\lambda'} = \frac{330128^2 + 3.110042^2}{2^2 + 3.1^2} = \frac{124775^2 + 3.41594^2}{1} = \frac{Z'}{\lambda}.$$

* *Conformal Division* means *division with preservation of 2^{ic} form.* See the author's Paper on "Connexion of Quadratic Forms" in *Proc. Lond. Math. Soc.*, Vol. XXVIII., 1897, for a full explanation of the process.

Reducing the fractions by the Rules of "conformal division,"

$$Z/\lambda' = 47161^2 + 3.78602^2 = 124775^2 + 3.115942^2 = Z'/\lambda,$$
$$= \quad A^2 \quad + \quad 3B^2 \quad = \quad A'^2 \quad + \quad 3B'^2$$

whence $\quad \dfrac{\eta_1}{\theta_1} = \dfrac{A'+A}{B-B'} = \dfrac{77614}{37008} = \dfrac{151}{72}; \quad \dfrac{\eta_2}{\theta_2} = \dfrac{A'+A}{B+B'} = \dfrac{77614}{120196} = \dfrac{257}{398}.$

Hence,

$L = 151^2 + 3.72^2 = 38353 = 7.5479; \quad M = 257^2 + 3.398^2 = 541281 = 7.77323;$

And, finally, $\quad N = 1.7;\ 7.5479 : 7.77323.$

21. *Aurifeuillians.* These are numbers of type

$$N = (X^q \pm Y^q) \div (X \pm Y), \quad \text{with } X = \xi^2, \quad Y = q\eta^2 \text{ ....(64).}$$

When q is an odd prime—(as in the present Paper)—there are two types of Aurifeuillians, each of which is *algebraically* expressible as a difference of squares, and thereby resolvable into two co-factors (L, M),

i. $N = (X^q + Y^q) \div (X + Y) = P^2 - Q^2$, when $q = 4k + 3$.........(64a),

ii. $N = (X^q - Y^q) \div (X - Y) = P^2 - Q^2$, when $q = 4k + 1$.........(64b),

and, in both cases,

$$N = P^2 - Q^2 = L.M; \quad L = P - Q, \quad M = P + Q \text{.................(65).}$$

The two co-factors L, M—styled* *Aurifeuillian Factors*—have the properties of being *mutually prime*, and of being *algebraically* expressible in the same 2^{ic} forms as N itself.

The only case of type i which is algebraically convertible into a Quasi-Mersennian $N = (x^q - y^q)$ occurs with $q = 3$ (this is treated of in Art. 22): but all cases of type ii. yield Quasi-Mersennians (these are treated of in Art. 23—23*b*).

22. *Trin-Aurifeuillians.* These are numbers of form

$$N = (\xi^6 + 3^3.\eta^6) \div (\xi^2 + 3\eta^2) \text{ ....(66),}$$

and are *algebraically* expressible as a difference of squares

$$N = (\xi^2 + 3\eta^2)^2 - (3\xi\eta)^2 = P^2 - Q^2 \text{.........................(67),}$$

and are therefore immediately resolvable into the two co-factors L, M

$$N = L.M, \text{ where } L = P - Q, \quad M = P + Q \text{ ....(68).}$$

Now, taking $q = 3$, the Quasi-Mersennian (N_3) is a *Cuban*, which is *algebraically* expressible in the forms (29)

$$N_3 = \frac{x^3 - y^3}{x - y} = \frac{(x+y)^3 + x^3}{(x+y) + x} = \frac{(x+y)^3 + y^3}{(x+y) + y}; \quad [x - y = 1] \text{.........(69),}$$

* In the numerical examples which follow (Art. 22, 23*d*), these factors (L, M) are separated by a colon (thus $L : M$).

and the last of these forms will be a Trin-Aurifeuillian* in two cases, given by

i. $x+y=3\eta^2,\ y=\xi^2$	ii. $x+y=\xi^2,\quad y=3\eta^2$ ....(70*a*),
whence $x=3\eta^2-\xi^2$	whence $x=\xi^2-3\eta^2$ ....(70*b*),
and $x-y=3\eta^2-2\xi^2=+1$	and $x-y=\xi^2-6\eta^2=+1$ ....(70*c*),

and every solution (ξ, η) of these last two Pellian forms (70*c*) converts N_3 into the Trin-Aurifeuillian (66) with the two co-factors L, M.

Ex. The Table below shows the successive solutions (ξ, η) of the two Pellians (70*c*), the corresponding elements (x, y) of the Quasi-Mersennian (N) and the co-factors (L, M) of the same thence resulting, resolved into prime factors.

$3\eta^2-2\xi^2=1$	$r=$	0	2	4	6
	ξ, η	1, 1	11, 9	109, 89	1079, 881
	x, y	2, 1	122, 121	11882, 11881	1164242, 1164241
	L, M	1 : 7 ;	67 : 661 ;	31.211 : 64747 ;	7.19.61.79 : 43.147547 ;
$\xi^2-6\eta^2=+1$	$r=$	1	3	5	7
	ξ, η	5, 2	49, 20	485, 198	4801, 1960
	x, y	13, 12	1201, 1200	117613, 117612	11524801, 11524800
	L, M	7 : 67 ;	661 : 31.211 ;	64747 : 7.19.61.79 ;	43.147547 : 37.1697413 ;

22*a*. *Trin-Aurifeuillian Chain.* If the successive solutions (ξ_r, η_r) of the two Pellians be distinguished by subscripts, thus—

$$(\xi_0, \eta_0),\ (\xi_2, \eta_2),\ (\xi_4, \eta_4),\ (\xi_6, \eta_6),\ \ldots,\ \text{of}\ 3\eta^2-2\xi^2=1,$$
$$(\xi_1, \eta_1),\ (\xi_3, \eta_3),\ (\xi_5, \eta_5),\ (\xi_7, \eta_7),\ \ldots,\ \text{of}\ \xi^2-6\eta^2=1,$$

and, if similar subscripts be attached to the corresponding elements (x, y), and to the co-factors (L, M), and to the whole numbers N, it will be seen that the *successive* factors, (L, M), taken *one from each series alternately* are connected by a "Chain" relation, thus—

$$\ldots,\ M_{2r}=L_{2r+1},\ M_{2r+1}=L_{2r+2},\ \ldots,\ \text{and so on} \quad\text{.................(71).}$$

23. *Aurifeuillians* $(q=4k+1)$. All primes (q) of form $q=4k+1$ yield Aurifeuillians of order q, *i.e.* numbers of type

$$N=(X^q-Y^q)\div(X-Y),\ \text{with}\ X=\xi^2,\ Y=q\eta^2 \quad\text{..............(72),}$$

which admit of *algebraical* expression as a difference of squares, and are therefore immediately resolvable into two co-factors (L, M),

$$N=P^2-Q^2=L.M;\quad L=P-Q,\ M=P+Q \quad\text{..................(73),}$$

* It will be seen that the convertibility of $N=(x^3-y^3)$ into a Trin-Aurifeuillian (66), in which the connecting sign is +, is due to the relation (69) which is a property peculiar to Cubans.

The Quasi-Mersennian ($N_q = x^q - y^q$) may become an Aurifeuillian of the same order (q) in two ways, viz. when

i. $x = q\eta^2,\ y = \xi^2$	ii. $x = \xi^2,\ y = q\eta^2$ ....(74*a*),
whence $x - y = q\eta^2 - \xi^2 = 1$	whence $x - y = \xi^2 - q\eta^2 = 1$ ....(74*b*).

All solutions (ξ, η) of these two Pellian forms (with $q = 4k + 1$, a prime), give rise to Aurifeuillian forms of the Quasi-Mersennians.

23*a*. *Quint-Aurifeuillians* ($q = 5$). The formulæ required for factorisation are—

Case i. $x = 5\eta^2,\ y = \xi^2$	Case ii. $x = \xi^2,\ y = 5\eta^2$ ......(75*a*),
$x - y = \xi^2 - 5\eta^2 = -1$	$x - y = \xi^2 - 5\eta^2 = +1$....(75*b*).

In both Cases $P = x^2 + 3xy + y^2$, $Q = 5\xi\eta(x + y)$...(76).

23*b*. *Aurifeuillians* ($q = 4k + 1 > 5$). The formulæ for P, Q are so long (when $q > 5$) that it does not seem worth while quoting them here, as the values of L, M are (almost at the start) too large for practical factorisation into prime factors.

23*c*. *Aurifeuillians* ($q = k^2 + 1$). This is a Sub-Case of the last. The Quasi-Mersennian

$$N_q = q^q - (q-1)^q = q^q - k^{2q} \text{ ....} (77)$$

is an Aurifeuillian of order q, and is *algebraically* resolvable into two co-factors (L, M). Examples of the Cases $q = 5$, 17 are given below. Other cases $q = 37$, 101, &c., give L, M too large for practical work.

23*d*. *Aurifeuillians* ($q = F_n$). If $E_n = 2^{2^n}$, and $F_n = E_n + 1$, a Fermat's Number: then, taking $q = F_n$ (a prime > 3), the number

$$N_q = F^F - E^F, \quad [E, F \text{ having the } \textit{same subscript } n] \text{...} (78)$$

is an Aurifeuillian of order $q = F_n$, and is algebraically resolvable into two co-factors (L, M). Examples of the cases of $q = F_n = 5$, 17 are given below: other cases ($q = 257$, &c.) give L, M too large for practical work.

Examples. The Table below gives a few of the successive solutions (ξ, η) of the two Pellians (74*b*), the elements (x, y) and the co-factors L, M of the Aurifeuillian Quasi-Mersennian (N_q) thence formed, for $q = 5$, 13, 17;

[Several steps, $r=0$, 1, 2 are given for the case of $q=5$:

Only the starting case ($r=0$) is given for $q=13$, 17; as L, M are at once too large].

q	·	$r=$	0	1	2	·	0	1
5	$\xi^2-5\eta^2=\bar{1}$	ξ, η	2, 1	38, 17	682, 305	$\xi^2-5\eta^2=1$	9, 4	161, 72
		x, y	5, 4	1445, 1444	465125, 46124		81, 80	25921, 25920
		L	11;	1101431;			11.311	354657241?*
		M	191;	11.1796761;			61381	11.41.41.344171
13	$\xi^2-13\eta^2=\bar{1}$	ξ, η	18, 5			$\xi^2-13\eta^2=1$	649, 180	
		x, y	325, 324				421201, 421200	
		L	53.2204800458407 ? †					
		M	131.313.3698977215077 ? †					
17	$\xi^2-17\eta^2=\bar{1}$	ξ, η	4, 1			$\xi^2-17\eta^2=1$	33, 8	
		x, y	17, 16				1089, 1088	
		L	409.6891733;					
		M	613.307946161 ? †					

24. *Ant-Aurifeuillians* ($q=4k-1$). These are numbers of form

$$N=(\xi^{2q}-q^q.\eta^{2q})\div(\xi^2-q\eta^2), \quad [q=4k-1]\ldots\ldots(79),$$

which are *algebraically* expressible in the 2^{ic} form

$$N=P^2+Q^2, \text{ when } q=4k-1\ldots\ldots\ldots\ldots(80).$$

The Quasi-Mersennian (N_q) becomes of this form by taking

$$x=\xi^2, \; y=q\eta^2, \quad \text{with } x-y=\xi^2-q\eta^2=+1\ldots\ldots(81).$$

Every solution (ξ, η) of this last Pellian Equation—(which is always solvable)—gives rise to a Quasi-Mersennian (N_q), which is of same order (q), and algebraically expressible as a sum of squares.

The general algebraic formulæ for P, Q—which are rather lengthy in the general case—become comparatively simple in the present case upon reduction by the condition $x-y=1$; the reduced values of P, Q for the cases of $q \not> 19$ are given below

q	N	x	y	P	Q
3	x^3-y^3	ξ^2,	$3\eta^2$	1	$3\xi\eta$
7	x^7-y^7	ξ^2,	$7\eta^2$	1	$7\xi\eta(xy+1)$
11	$x^{11}-y^{11}$	ξ^2,	$11\eta^2$	$11x^2y^2-1$	$11\xi\eta(x^2y^2-3xy-1)$
19	$x^{19}-y^{19}$	ξ^2,	$19\eta^2$	$19x^2y^2(xy-1)^2-1$	$19\xi\eta(x^4y^4-2x^3y^3+7x^2y^2-5xy+1)$

† No more divisors <1000. * No divisors <101,

It will be seen that P, Q reduce to the forms

$$P = f_1(xy), \quad Q = q\xi\eta \cdot f_2(xy) \text{............} (82).$$

Ex. In the Table below are Examples for the orders $q=3, 7, 11$; giving the successive solutions (ξ, η) of the Pellian (81), and the elements (x, y) and 2ic parts P, Q of N_q from the above formulæ. The simple form of the results

$$N_q = x^q - y^q = 1^2 + Q^2, \quad \text{when } q = 3 \text{ or } 7 \text{.....................} (83),$$

is worth notice; but the numbers P, Q rise too rapidly, as ξ, η increase, to be of much use, except in the case of $q=3$.

$q=3$, $\xi^2-3\eta^2=1$	$r=$	1	2	3	4	5	6
	ξ, η	2, 1	7, 4	26, 15	97, 56	362, 209	1351, 780
	x, y	4, 3	49, 48	676, 675	9409, 9408	131044, 131043	1825201, 1825200
	P, Q	1, 6	1, 84	1, 1170	1, 16296	1, 226974	1, 3161340

$q=7$, $\xi^2-7\eta^2=1$	$r=$	1	2
	ξ, η	8, 3	127, 48
	x, y	64, 63	16129, 16128
	P, Q	1, 677544	1, 11100203906736

$q=11$, $\xi^2-11\eta^2=1$	$r=$	1
	ξ, η	10, 3
	x, y	100, 99
	P, Q	1078109999, 32333498670

25. *Sum of Squares.* Besides the case of Ant-Aurifeuillians (Art. 24), there are many cases in which a Quasi-Mersennian is expressible as a sum of squares (though *not algebraically*). This involves as a preliminary condition

$$N_q = 4n+1; \text{ whence } x = \epsilon, \; y = 4\eta - 1; \text{ or } x = 4\xi + 1, \; y = \epsilon \text{........} (83).$$

Hence $\quad N_q = \mathrm{a}^2 + \mathrm{b}^2$, if $N_q =$ a *prime* $p = 4\varpi + 1$ .... (84),

or $\; = \Pi(p)$, a product of such primes...(84*a*).

[Examples will be found in the Factorisation-Tables, Tab. II., III.]

26. *Equal Heteromorphs.* The question arises whether two Quasi-Mersennians of *different orders* $(q \neq q')$ can be equal. No general Rule is known, but the Example below shows the *possibility* of equality.

$$N_7 = 2^7 - 1 = 127 = 7^3 - 6^3 = N_3.$$

27. *Product of Quasi-Mersennians.* There are two cases in which the product of two *successive* Quasi-Mersennians is expressible in a quite simple form.

$$\text{Let } N_q = L_q \cdot M_q = (z^q - x^q)(x^q - y^q); \quad [z - x = 1 = x - y].$$

i. $\quad q=3; \quad \mathrm{N}_3 = \{(x+1)^3 - x^3\} \cdot \{x^3 - (x-1)^3\}$

$$= (3x^2 + 3x + 1)(3x^2 - 3x + 1) = 9x^4 - 3x^2 + 1$$

$$= (3^3x^6 + 1) \div (3x^2 + 1), \text{ a } \textit{Trin-Aurifeuillian} \text{........} (85).$$

ii. $\quad q=5; \quad \mathrm{N}_5 = \{(x+1)^5 - x^5\} \cdot \{x^5 - (x-1)^5\}$

$$= (5x^4 - 1)^2 - 5x^2 \text{..} (86).$$

Ex. of ii. $\;(6^5 - 5^5)(5^5 - 4^5) = (5^5 - 1)^2 - 5^3; \;\; (26^5 - 25^5)(25^5 - 24^5) = (5^9 - 1)^2 - 5^5.$

Divisors p *&* p^κ ($\not> 1000$) *of* $N_q = x^q - y^q$; **Tab. I.**

$[x - y = 1,\ q = a \text{ prime} > 3, \text{ but} < 50]$.

[Limit of x is $X = 50$, when $q = 5$; $X = 20$, when $q > 5$.]

p	q	x	X
11	5	4, 5, 7, 8	p
23	11	2, 3, 4, 9, 11, 13, 15, 20, 21, 22	p
29	7	3, 5, 6, 24, 25	25
31	5	2, 10, 22, 30	p
41	5	9, 12, 30, 33	p
43	7	14, 15, 20	20
47	23	2, 3, 4, 7, 8, 9, 11, 17, 18, 20	20
53	13	3, 7, 16, 20	20
59	29	4, 5, 11, 14, 16, 17, 20, 21, 22, 24	25
61	5	16, 24, 38, 46	50
67	11	12, 15, 17, 25, 32	32
71	5	4, 19	50
71	7	3, 16	20
79	13	5, 7, 15	20
83	41	4, 6, 10, 11, 12, 14, 15, 17, 19, 20	25
89	11	2, 7	20
101	5	27, 29	50
103	17	9, 12, 14, 19	20
113	7	15	20
127	7	2, 18	20
131	5	24	50
131	13	4, 19	20
137	17	6, 15	20
139	23	5, 18	20
149	37	6, 11, 12, 13, 15, 17	20
151	5	13, 43	50
157	13	8, 12	20
173	43	8, 20	20
181	5	None	50
191	5	5, 24	50
191	19	6, 9, 16	20
197	7	None	20
199	11	None	20
211	5	3, 44	50
	7	37	37
223	37	2, 8, 11, 15, 16, 17	20
229	19	17, 20	20
233	29	2, 11, 14, 15	20
239	7	None	20
239	17	10	20
241	5	14	50
251	5	39	50
271	5	30	50
277	23	10, 18	20
281	5	None	50
281	7	13, 18	20
283	47	10, 11, 16, 18	20
307	17	11	20

p	q	x	X
311	5	None	50
311	31	4, 6, 10	20
313	13	12	20
331	5	21	50
331	11	3, 17	20
337	7	None	20
349	29	4, 5, 16	20
353	11	19	20
373	31	20	20
379	7	None	20
397	11	None	20
401	5	96	96
409	17	6, 17	20
419	11	None	20
419	19	None	20
421	5	None	50
421	7	92	92
431	5	16	50
431	43	2, 3, 4, 9	20
443	13	13	20
443	17	6	20
449	7	None	20
457	19	None	20
461	5	None	50
461	23	11	20
463	7	14	20
463	11	None	20
491	5	None	50
491	7	43	43
521	5	None	50
521	13	45	45
523	29	16	20
541	5	23	50
547	7	None	20
547	13	15	20
571	5	None	50
571	19	19	20
593	37	None	20
599	13	17	20
599	23	5	20
601	5	48	50
613	17	10, 15, 17	20
617	7	None	20
617	11	None	20
631	5	None	50
631	7	None	100
641	5	9	50
647	17	None	20
647	19	13	20
659	7	None	20
659	47	15, 17	20
661	5	None	50

TAB. I.—*continued.*

p	q	x	X	p	q	x	X
661	11	None	100	883	7	None	20
673	7	None	20	911	5	None	50
677	13	15	20	911	7	20	20
683	11	None	20	911	13	76	76
683	31	18	20	919	17	None	20
691	5	14	50	929	29	None	20
691	23	None	100	937	13	11	20
701	5	None	100	941	5	None	50
701	7	38	38	941	47	22	22
727	11	12	20	947	11	None	20
739	41	None	20	947	43	None	20
743	7	None	20	953	7	None	20
751	5	19	50	953	17	None	20
757	7	None	20	967	7	None	20
761	5	None	50	967	23	None	20
761	19	50	50	971	5	None	50
811	5	13	50	991	5	None	50
821	5	7	50	991	11	23	23
821	41	3, 5, 6, 20	20				
827	7	None	20	p^κ	q	x	X
829	23	None	20				
859	11	None	20	11^2	5	15	50
859	13	None	20	23^2	11	3	20
881	5	34	50	29^2	7	None	20
881	11	57	57	31^2	5	None	50

Factorisation of $N = (x^q - y^q)$; TAB. IV.

$[x - y = 1,\ x \ngtr 12;\ q = \textit{prime} > 13 \textit{ up to } 47]$.

[† shows all divisors $< 10^3$ cast out; ‡ shows all divisors $< 10^4$ cast out].

q	$(3^q - 2^q)$‡	$(4^q - 3^q)$‡	$(5^q - 4^q)$‡	$(6^q - 5^q)$†
17	129009061?		1259.2381.248779;	137.409.443.651169;
19	1559.745181;			191;
23	47.	47.1933.77351488 7?	139.599.	
29		59.349.	59.349.6091.	
31		311.		311.
37				149.
41	821.	83.	821.	83.821.
43	431.	431.		
47	1129.			

q	$(7^q - 6^q)$†	$(8^q - 7^q)$‡	$(9^q - 8^q)$‡	$(10^q - 9^q)$†	$(11^q - 10^q)$†	$(12^q - 11^q)$†
17			103.	239.613.	307.	103.
19			191.			
23	47.	47.	47.	277.	47.461.	
29					59.233.	
31				311.		
37	2887.	223.			149.223.	149.
41				83.	83.1231.	83.
43		173.	431.			
47				283.	283.	

Cuban Primes. TAB. II.

$p=(x^3-y^3)\div(x-y)$ up to $p \not> 10^6$, $[x-y=1]$.

p	x	p	x	p	x	p	x
1	1	35317	109	202021	260	590077	444
7	2	42841	120	213067	267	592741	445
19	3	45757	124	231019	278	595411	446
37	4	47251	126	234361	280	603457	449
61	5	49537	129	241117	284	608851	451
127	7	50311	130	246247	287	611557	452
271	10	55897	137	251431	290	619711	455
331	11	59221	141	260191	295	627919	458
397	12	60919	143	263737	297	650071	466
547	14	65209	148	267307	299	658477	469
631	15	70687	154	276337	304	666937	472
919	18	73477	157	279991	306	689761	480
1657	24	74419	158	283669	308	692641	481
1801	25	75367	159	285517	309	698419	483
1951	26	81181	165	292969	313	707131	486
2269	28	82171	166	296731	315	733591	495
2437	29	87211	171	298621	316	742519	498
2791	31	88237	172	310087	322	760537	504
3169	33	89269	173	329677	332	769627	507
3571	35	92401	176	333667	334	772669	508
4219	38	96661	180	337681	336	784897	512
4447	39	102121	185	347821	341	791047	514
5167	42	103231	186	351919	343	812761	521
5419	43	104347	187	360187	347	825301	525
6211	46	110017	192	368551	351	837937	529
7057	49	112327	194	372769	353	847477	532
7351	50	114661	196	374887	354	863497	537
8269	53	115837	197	377011	355	879667	542
9241	56	126691	206	383419	358	886177	544
10267	59	129169	208	387721	360	895987	547
11719	63	131671	210	398581	365	909151	551
12097	64	135469	213	407377	369	915769	553
13267	67	140617	217	423001	376	925741	556
13669	68	144541	220	436627	382	929077	557
16651	75	145861	221	452797	389	932419	558
19441	81	151201	225	459817	392	939121	560
19927	82	155269	228	476407	399	952597	564
22447	87	163567	234	478801	400	972991	570
23497	89	169219	238	493291	406	976411	571
24571	91	170647	239	522919	418	986707	574
25117	92	176419	243	527941	420	990151	575
26227	94	180811	246	553411	430	997057	577
27361	96	189757	252	574219	438		
33391	106	200467	259	584767	442		

TAB. III.

Factorisation of $N_q = (x^q - y^q)$; $[x - y = 1;\ q = 5, 7, 11, 13]$.

[† shows all divisors < 10^3 cast out; ‡ shows all divisors < 10^4 cast out.].

x	x^5-y^5	x^7-y^7	$x^{11}-y^{11}$	$x^{13}-y^{13}$
2	31;	127;	23.89;	8191;
3	211;	29.71;	23.23.331;	53.29927;
4	11.71;	14197;	23.174659;	131.500111;
5	11:191;	29.2129;	6359.7019;	79.14602459? ‡
6	4651;	29.6959;	†	†
7	11.821;	543607;	89.18140783 †	53.79.20021093?†
8	11.1451;	1273609;	‡	157.3329 866477;
9	41.641;	2685817;	23. ‡	‡
10	31.1321;	5217031;	†	†
11	61051;	1499.6329;	23. †	937. †
12	41.2141;	10344637? †	67.727.9396553;	157.313. †
13	151.811;	281.95789;	23. †	443. †
14	241.691;	43.463.2143;	†	†
15	121.1831;	43.113.13469.	23.67. †	79.547.677. †
16	11.61.431;	71 1374311;	†	53. †
17	371281;	†	67.331. †	599. †
18	11.42701;	127.281.5657;	†	†
19	11.71.751;	†	353. †	131. †
20	723901;	43.911.9857;	23. †	53. †
21	331.2671;		23.	
22	31.34501;		23.	
23	541 2371;			
24	61.131.191;	29.		
25	1803001;	29.	23 67.	

x	x^5-y^5	x	x^5-y^5	x	x^5-y^5
26	11 192341;	35	7086451;	43	151.108061;
27	11.101.2221;	36	7944301;	44	211.84871;
28	2861461;	37	11.807071;	45	19611901? †
29	11.101 2971;	38	11.61.14741;	46	61.351391;
30	11.31.41 271;	39	251.43781;	47	23382031? †
31	4329151;	40	11.1106891;	48	11.601.3851;
32	4925281;	41	11 31.39461;	49	11.2515571;
33	31.41.4391;	42	14835031? †	50	41.732311;
34	881.7151;				

Corrigenda for Jacobi's "Canon Arithmeticus."

[In addition to those in the printed Work.]

Tabula Numerorum.

Pag.	*p*	*Arg.*	*Loco.*	*Lege.*
62	457	453	325	320
63	461	$p-1$	2^4	2^2
76	523	$p-1$	2.3.87	$2.3^2.29$
77	523	$p-1$	2.3.87	$2\ 3^2.29$
155	821	328	4 0	470
193	929	91	*Argum.*	90
,,	,,	92	*mutandum*	91
,,	,,	93		92
225	243	12	206	208
228	361	131	169	165
234	841	192	233	223

Tabula Indicum.

Pag.	*p*	*Arg.*	*Loco.*	*Lege.*
139	757	500	19	419
140	757	568	168	468
222	25	14	8	6
224	169	33	41	71
228	361	122	43	93
,,	,,	216	87	78
,,	,,	353	144	74
232	729	196	204	304
234	841	353	394	694
	Dele	*Corri*	*gendum*	
85	571	109	190*	109

* The original 190 is correct.

ON SYMMETRIC AND ORTHOGONAL SUBSTITUTIONS.

By *Harold Hilton.*

Abstract.

(1) Any given symmetric substitution can be transformed by means of an orthogonal substitution into the direct product of symmetric substitutions, each of which has only a single invariant-factor.

(2) Any given orthogonal substitution can be transformed by means of an orthogonal substitution into the direct product of orthogonal substitutions, each of which has either (i) a pair of invariant-factors $(\lambda-\alpha)^r$ and $(\lambda-1/\alpha)^r$, where $\alpha^2\neq 1$, or (ii) a single invariant-factor $(\lambda-1)^r$ or $(\lambda+1)^r$, where r is odd, or (iii) a pair of invariant factors $(\lambda-1)^r$ and $(\lambda-1)^r$ or $(\lambda+1)^r$ and $(\lambda+1)^r$, where r is even.

§ 1. We shall use the following notation:—
The substitution of degree m

$$x_t'=p_{t1}x_1+p_{t2}x_2+\dots+p_{tm}x_m \quad (t=1,\ 2,\ \dots,\ m),$$

whose coefficients involve the letter p, will be denoted by the capital letter P, while the bilinear form

$$\Sigma p_{ij} y_i x_j \quad (i, j, = 1, 2, \ldots, m)$$

will be denoted by $p(x, y)$. The substitution transposed to P will be denoted by P'.

If D is any substitution, DD' is symmetric; and, conversely, D can be chosen so that $DD' = A$, where A is any given symmetric substitution so that $a_{ij} = a_{ji}$.

That DD' is symmetric is at once seen on forming the product of D and D'. The converse is established thus:—

Suppose that $a(x, x)$, when expressed as the sum of m squares, takes the form

$$(d_{11}x_1 + d_{12}x_2 + \ldots + d_{1m}x_m)^2 + (d_{21}x_1 + \ldots + d_{2m}x_m)^2 + \ldots$$
$$+ (d_{m1}x_1 + \ldots + d_{mm}x_m)^2.$$

Then the required substitution is D. For it is at once verified that if B is *any* substitution and in $b(x, y)$, etc., we put

$$p_{t1}x_1 + p_{t2}x_2 + \ldots + p_{tm}x_m \text{ for } x_t,$$
$$q_{t1}y_1 + q_{t2}y_2 + \ldots + q_{tm}y_m \text{ for } y_t,$$

we get $c(x, y)$, where $C = PBQ'$.

Take $P = Q = D$, $B = E$ (the identical substitution $x_t' = x_t$). Then we get $A = DED' = DD'$, which was to be proved.

§ 2. If N is any substitution transformed by P into a *symmetric* substitution A so that $P^{-1}NP = A$, then $N.PP'$ is symmetric; and, conversely, if $N.PP'$ is symmetric, so is A. For if A is symmetric, $NP = PA$ gives

$$p_{t1}n_{1j} + p_{t2}n_{2j} + \ldots + p_{tm}n_{mj} = a_{t1}p_{1j} + a_{t2}p_{2j} + \ldots + a_{tm}p_{mj}$$
$$(t = 1, 2, \ldots, m).$$

Therefore, if $PP' = C$, so that

$$c_{ij} = c_{ji} = p_{1i}p_{1j} + p_{2i}p_{2j} + \ldots + p_{mi}p_{mj},$$

$$\begin{aligned}
c_{i1}n_{1j} &+ \ldots + c_{im}n_{mj} \\
&= \Sigma p_{ti}(p_{t1}n_{1j} + \ldots + p_{tm}n_{mj}) \\
&= \sum_t p_{ti}(a_{t1}p_{1j} + \ldots + a_{tm}p_{mj}) \\
&= \sum_t p_{ti}(a_{1t}p_{1j} + \ldots + a_{mt}p_{mj}) \\
&= p_{1j}\sum_t a_{1t}p_{ti} + \ldots + p_{mj}\sum_t a_{mt}p_{ti} \\
&= p_{1j}(p_{11}n_{1i} + \ldots + p_{1m}n_{mi}) + \ldots + p_{mj}(p_{m1}n_{1i} + \ldots + p_{mm}n_{mi}) \\
&= c_{j1}n_{1i} + \ldots + c_{jm}n_{mi}.
\end{aligned}$$

Therefore NC is symmetric. Conversely, if NC is symmetric, the above argument gives

$$\sum_{t,s} p_{ti} p_{sj} (a_{st} - a_{ts}) = 0 \quad (i, j = 1, 2, \ldots, m).$$

The determinant of these m^2 linear equations in the m^2 quantities $(a_{st} - a_{ts})$ is not zero, for it is the $2m^{\text{th}}$ power of the determinant of P. Therefore each of the quantities $(a_{st} - a_{ts})$ is zero, or A is symmetric.

As a particular case of this, suppose P orthogonal. Then $C = E$, and N is symmetric if A is. Hence the transform of a symmetric substitution by an orthogonal substitution is symmetric, as is well known.

Take now N as the "canonical" substitution

$$\left.\begin{array}{l} x_t' = \lambda_t x_t + \beta_t x_{t+1} \quad (t = 1, 2, \ldots, m) \\ \text{where } \beta_t = 0 \text{ or } 1, \text{ being always } 0 \text{ if } \lambda_t \neq \lambda_{t+1} \ (\beta_0 = \beta_m = 0) \end{array}\right\}$$

into which A can be always transformed.* Then we have

$$\lambda_i c_{ij} + \beta_{i-1} c_{i-1\,j} = \lambda_j c_{ij} + \beta_{j-1} c_{i\,j-1},$$

or at greater length

$$\left.\begin{array}{l} (\lambda_i - \lambda_1)\, c_{i1} + \beta_{i-1} c_{i-1\,1} = 0 \\ (\lambda_i - \lambda_2)\, c_{i2} + \beta_{i-1} c_{i-1\,2} = \beta_1 c_{i1} \\ (\lambda_i - \lambda_3)\, c_{i3} + \beta_{i-1} c_{i-1\,3} = \beta_2 c_{i2} \\ \quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ (\lambda_i - \lambda_m)\, c_{im} + \beta_{i-1} c_{i-1\,m} = \beta_{m-1} c_{i\,m-1} \end{array}\right\} \quad (i = 1, 2, \ldots, m).$$

From these we readily deduce:—

If $\lambda_i \neq \lambda_j$, then $c_{ij} = 0$. If $\lambda_i = \lambda_j$, then $\beta_{i-1} c_{i-1\,j} = \beta_{j-1} c_{i\,j-1}$, so that,

$$\text{if } \beta_{i-1} = 1 \text{ and } \beta_{j-1} = 0,\ c_{i-1\,j} = 0;$$

$$\text{if } \beta_{i-1} = 0 \text{ and } \beta_{j-1} = 1,\ c_{i\,j-1} = 0;$$

$$\text{if } \beta_{i-1} = 1 \text{ and } \beta_{j-1} = 1,\ c_{i-1\,j} = c_{i\,j-1}.$$

For example, if N is

$$\left.\begin{array}{llll} x_1' = \alpha x_1 + x_2, & x_2' = \alpha x_2 + x_3, & x_3' = \alpha x_3, & x_4' = \alpha x_4 + x_5 \\ x_5' = \alpha x_5, & x_6' = \alpha x_6 + x_7, & x_7' = \alpha x_7, & x_8' = \alpha x_8. \end{array}\right\},$$

* *Messenger of Math.*, vol. XXXIX., p. 24.

C has a matrix of the type

$$\left|\begin{array}{cccccccc} 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & a & b & 0 & d & 0 & f & 0 \\ a & b & c & d & e & f & g & h \\ 0 & 0 & d & 0 & i & 0 & k & 0 \\ 0 & d & e & i & j & k & l & m \\ 0 & 0 & f & 0 & k & 0 & n & 0 \\ 0 & f & g & k & l & n & p & q \\ 0 & 0 & h & 0 & m & 0 & q & r \end{array}\right|,$$

from which the general form of C is clear.

N is the direct product of substitutions on x_1, x_2, x_3; on x_4, x_5; on x_6, x_7; and on x_8. We shall say that the variables of N form the *sets* (x_1, x_2, x_8), (x_4, x_5), (x_6, x_7), (x_8).

§3. We now proceed to show that *any given symmetric substitution A can be transformed by means of an orthogonal substitution into the direct product of symmetric substitutions, each of which has only a single invariant-factor.**

If A is *real*, the exponent of each invariant-factor is unity. This will not necessarily be the case if A is unreal. The theorem is an extension of a result proved in a previous paper.†

Suppose $P^{-1}NP = A$, where N is the canonical form of A; and let $PP' = C$.

(i) First we show that A may be transformed by an orthogonal substitution into a symmetric substitution which is the direct product of substitutions, each of which has only one distinct characteristic-root ‡

Using the statement "If $\lambda_i \neq \lambda_j$, then $c_{ij} = 0$" of §2, we see that C is the direct product of substitutions each

---

* Whose canonical form is therefore of the type

$$x_1' = ax_1 + x_2, \ \ldots, \ x'_{r-1} = ax_{r-1} + ax_r, \ x_r' = ax_r;$$

the invariant-factor being $(\lambda - a)^r$.

† *Proc. Lond. Math. Soc.*, 2, x. (1911), p. 277.

‡ The "characteristic-roots" of P are the roots of the equation in λ:

$$\left|\begin{array}{cccc} p_{11} - \lambda & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} - \lambda & \cdots & p_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ p_{m1} & p_{m2} & \cdots & p_{mm} - \lambda \end{array}\right| = 0.$$

of which affects only the variables corresponding to a single characteristic-root of N.

By § 1 we can choose a direct product D of substitutions on the same groups of variables so that $DD' = C^{-1}$. Then $D'P$ is orthogonal, for

$$(D'P)(D'P)' = D'PP'D = D'CD = D^{-1}D = E.$$

Also the orthogonal substitution $(D'P)^{-1}$ transforms A into the direct product of substitutions each affecting only variables corresponding to a single characteristic-root of N, since

$$(D'P)A(D'P)^{-1} = D'PAP^{-1}D'^{-1} = D'ND'^{-1},$$

and both D' and N are such direct products.

(ii) We may therefore now confine our attention to a substitution A which has only a single distinct characteristic-root.

Take B as a substitution permutable with N such that $H \equiv BCB'$ is symmetric and is the direct product of substitutions each affecting one "set" (§ 2) of the variables of N. That B can be so chosen will be proved in § 4

Take now (§ 1) F so that $FF' = H^{-1}$, where F is the direct product of substitutions each affecting one set of the variables of N. Then $F'BP$ is orthogonal, for

$$(F'BP)(F'BP)' = F'BPP'B'F = F'BCB'F = F'HF = E.$$

Also the orthogonal substitution $(F'BP)^{-1}$ transforms A into the direct product of substitutions each affecting one set of the variables of N, since

$$\begin{aligned}(F'BP)A(F'BP)^{-1} &= F'BPAP^{-1}B^{-1}F'^{-1}\\ &= F'BNB^{-1}F'^{-1} = F'NF'^{-1},\end{aligned}$$

and both F' and N are such direct products.

§ 4. It now remains to prove that we can choose B permutable with N so that BCB' is symmetric and the direct product of substitutions each affecting one set of the variables of N.

$H = BCB' = BP.P'B' = QQ'$ (where $Q = BP$), and is therefore symmetric whatever B may be.

If B is *any* substitution permutable with N,

$$Q^{-1}NQ = P^{-1}B^{-1}NBP = P^{-1}NP = A,$$

so that $H(=QQ')$ is of the same type as C, *i.e.*, we have the equations

$$\lambda_i h_{ij} + \beta_{i-1} h_{i-1\,j} = \lambda_j h_{ij} + \beta_{j-1} h_{i\,j-1}$$

corresponding to

$$\lambda_i c_{ij} + \beta_{i-1} c_{i-1\,j} = \lambda_j c_{ij} + \beta_{j-1} c_{i\,j-1} \quad \text{of § 2.}$$

Now, by § 1, $h(x, x)$ is obtained by putting

$$b_{t1}x_1 + b_{t2}x_2 + b_{t3}x_3 + \ldots \text{ for } x_t$$

in $c(x, x)$; and we have to choose B permutable with N so that $h(x, x)$ is the sum of quadratic forms, each affecting the variables of one set of N.

The method will be clear from the following example:—

Suppose N is

$$x_1' = ax_1 + x_2, \quad x_2' = ax_2 + x_3, \quad x_3' = ax_3;$$
$$x_4' = ax_4 + x_5, \quad x_5' = ax_5 + x_6, \quad x_6' = ax_6,$$

and C has the matrix

$$\begin{vmatrix} 0 & 0 & r_{11} & 0 & 0 & r_{12} \\ 0 & r_{11} & s_{11} & 0 & r_{12} & s_{12} \\ r_{11} & s_{11} & t_{11} & r_{12} & s_{12} & t_{12} \\ 0 & 0 & r_{21} & 0 & 0 & r_{22} \\ 0 & r_{21} & s_{21} & 0 & r_{22} & s_{22} \\ r_{21} & s_{21} & t_{21} & r_{22} & s_{22} & t_{22} \end{vmatrix},$$

where $r_{12} = r_{12}$, $s_{12} = s_{12}$, $t_{12} = t_{12}$.

For x_1 put $l_{11}x_1 + l_{12}x_4$, for x_4 put $l_{21}x_1 + l_{22}x_4$.
for x_2 put $l_{11}x_2 + l_{12}x_5$, for x_5 put $l_{21}x_2 + l_{22}x_5$.
for x_3 put $l_{11}x_3 + l_{12}x_6$, for x_6 put $l_{21}x_3 + l_{22}x_6$.

This will not alter N.*

Choose the l's so that, when we put $l_{11}x_1 + l_{12}x_2$ for x_1 and $l_{21}x_1 + l_{22}x_2$ for x_2, $r_{11}x_1^2 + 2r_{12}x_1x_2 + r_{22}x_2^2$ reduces to $x_1^2 + x_2^2$. This is possible, for the determinant of C is $\begin{vmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{vmatrix}^3$, so that $\begin{vmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{vmatrix} \neq 0$. Then $c(x, x)$ becomes a quadratic form with a matrix of the type

$$\begin{vmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & \mathfrak{s}_{11} & 0 & 0 & \mathfrak{s}_{12} \\ 1 & \mathfrak{s}_{11} & \mathfrak{t}_{11} & 0 & \mathfrak{s}_{12} & \mathfrak{t}_{12} \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \mathfrak{s}_{21} & 0 & 1 & \mathfrak{s}_{22} \\ 0 & \mathfrak{s}_{21} & \mathfrak{t}_{21} & 1 & \mathfrak{s}_{22} & \mathfrak{t}_{22} \end{vmatrix},$$

where $\mathfrak{s}_{12} = \mathfrak{s}_{21}$, $\mathfrak{t}_{12} = \mathfrak{t}_{21}$.

Now put $x_1 - \mathfrak{s}_{12}x_5$ for x_1, $x_2 - \mathfrak{s}_{12}x_6$ for x_2. This will not alter N,* but it reduces $c(x, x)$ to a form with a matrix of the type

$$\begin{vmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & S_{11} & 0 & 0 & 0 \\ 1 & S_{11} & T_{11} & 0 & 0 & T_{12} \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & S_{22} \\ 0 & 0 & T_{21} & 1 & S_{22} & T_{22} \end{vmatrix},$$

where $T_{12} = T_{21}$.

Now put $x_1 - T_{12}x_6$ for x_1. This will not alter N,* while $c(x, x)$ is reduced to a form of the required type.

The method of this example is readily generalized.

§ 5. We now prove the corresponding theorem when A is orthogonal instead of symmetric, namely:—

Any given orthogonal substitution A can be transformed by means of an orthogonal substitution into the direct product of orthogonal substitutions each of which has either (1) *a pair of invariant-factors* $(\lambda - \alpha)^r$ *and* $(\lambda - 1/\alpha)^r$, *where* $\alpha^2 \neq 1$, *or* (2) *a single invariant-factor* $(\lambda - 1)^r$ *or* $(\lambda + 1)^r$, *where r is odd, or* (3) *a pair of invariant-factors* $(\lambda - 1)^r$ *and* $(\lambda - 1)^r$ *or* $(\lambda + 1)^r$ *and* $(\lambda + 1)^r$, *where r is even.*

If A is real, r is always unity.

The theorem is an extension of a result proved† in a former paper. [*Proc. London Math. Soc.*, 2, x. (1911), pp. 423–445.] In this paper we have established the following results:—

Suppose $P^{-1}NP = A$, where A is the canonical form of A, and let $PP' = C$. Then $c(x, x)$ is an invariant of N.‡ It follows that $c_{ij} = 0$ unless $\lambda_i\lambda_j = 1$. Hence, as in § 3 (i), we may confine our attention to the cases in which A has a pair of characteristic-roots α and $1/\alpha$, where $\alpha^2 \neq 1$, or a single characteristic-root $+1$ or -1.

The argument of § 3 (ii) still applies, except that we must choose B permutable with N so that $h(x, x)$, which is again an invariant of BNB^{-1} or N, is the sum of quadratic forms each affecting either (1) two "sets" of variables of N corresponding to invariant-factors $(\lambda - \alpha)^r$ and $(\lambda - 1/\alpha)^r$, or (2)

---

* See "On substitutions permutable with a canonical substitution," *Messenger of Math.*, vol. XLI., p. 110.

† *Loc. cit.*, p. 433.

‡ *Loc. cit.*, p. 423; since $x_1^2 + x_2^2 + \ldots + x_m^2$ is an invariant of A.

one set of variables corresponding to $(\lambda \pm 1)^r$, where r is odd, or (3) two sets of variables each corresponding to the invariant-factors $(\lambda - 1)^r$ or to $(\lambda + 1)^r$, where r is even.*

§ 6. We now justify this choice of B.

(1) If A has a pair of characteristic-roots α and $1/\alpha$, where $\alpha^2 \neq 1$, this has been done in *loc. cit.* § 12, see especially the footnote on p. 445. (The expression given at the top of p. 445 is not quite correct; but the argument is not affected thereby.)

(2) Suppose A has a single characteristic-root ± 1. Take, for example, N as in § 4 with $\alpha = 1$. Then (*loc. cit.* p. 428) the symmetric matrix of C takes the form

$$\begin{vmatrix} 0 & 0 & r_{11} & 0 & 0 & r_{12} \\ 0 & -r_{11} & * & 0 & -r_{12} & * \\ r_{11} & * & * & r_{12} & * & * \\ 0 & 0 & r_{21} & 0 & 0 & r_{22} \\ 0 & -r_{21} & * & 0 & -r_{22} & * \\ r_{21} & * & * & r_{22} & * & * \end{vmatrix},$$

where $r_{12} = r_{21}$, and the asterisks denote quantities not necessarily zero.

The argument is now much the same as in § 4.

(3) Take, for another example, N as

$$\left.\begin{array}{l} x_1' = x_1 + x_2,\ x_2' = x_2,\ x_3' = x_3 + x_4,\ x_4' = x_4 \\ x_5' = x_5 + x_6,\ x_6' = x_6,\ x_7' = x_7 + x_8,\ x_8' = x_8 \end{array}\right\}.$$

Then the symmetric matrix of C takes the form

$$\begin{vmatrix} 0 & 0 & 0 & r_{12} & 0 & r_{13} & 0 & r_{14} \\ 0 & * & -r_{12} & * & -r_{13} & * & -r_{14} & * \\ 0 & r_{21} & 0 & 0 & 0 & r_{23} & 0 & r_{24} \\ -r_{21} & * & 0 & * & -r_{23} & * & -r_{24} & * \\ 0 & r_{31} & 0 & r_{32} & 0 & 0 & 0 & r_{34} \\ -r_{31} & * & -r_{32} & * & 0 & * & -r_{34} & * \\ 0 & r_{41} & 0 & r_{42} & 0 & r_{43} & 0 & 0 \\ -r_{41} & * & -r_{42} & * & -r_{43} & * & 0 & * \end{vmatrix},$$

where $r_{ij} = -r_{ji}$.

* The number of sets corresponding to $(\lambda \pm 1)^r$, where r is even, is itself even *loc. cit.*, p. 432; or see Muth's *Elementartheiler*, p. 173.

Put
$$l_{11}x_1 + l_{12}x_3 + l_{13}x_5 + l_{14}x_7 \text{ for } x_1,$$
$$l_{11}x_2 + l_{12}x_4 + l_{14}x_6 + l_{24}x_8 \text{ for } x_2,$$
$$l_{21}x_1 + l_{22}x_3 + l_{23}x_5 + l_{24}x_7 \text{ for } x_3,$$
$$\&c. \qquad\qquad \&c.$$

as in § 4, the l's being chosen so that, when we put
$$l_{t1}x_1 + l_{t2}x_2 + l_{t3}x_3 + l_{t4}x_4 \text{ for } x_t,$$
$$l_{t1}y_1 + l_{t2}y_2 + l_{t3}y_3 + l_{t4}y_4 \text{ for } y_t,$$
the alternate bilinear form $\Sigma r_{ij} y_i x_j$ reduces to
$$(y_1x_2 - y_2x_1) + (y_3x_4 - y_4x_3) + (y_5x_6 - y_6x_5) + (y_7x_8 - y_8x_7).*$$
Then the matrix of C takes the form
$$\begin{vmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & * & -1 & * & 0 & * & 0 & * \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & * & 0 & * & 0 & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & * & 0 & * & 0 & * & -1 & * \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & * & 0 & * & 1 & * & 0 & * \end{vmatrix},$$
and now the argument is much the same as in § 4.

---

* See, *e.g.*, *Proc. Lond. Math. Soc.*, xxxii., p. 332.

ON AN ABSOLUTE CRITERION FOR FITTING FREQUENCY CURVES.

By *R. A. Fisher*, Gonville and Caius College, Cambridge.

1. If we set ourselves the problem, in its essence one of frequent occurrence, of finding the arbitrary elements in a function of known form, which best suit a set of actual observations, we are met at the outset by an arbitrariness which appears to invalidate any results we may obtain. In the general problem of fitting a theoretical curve, either to an observed curve, or to an observed series of ordinates, it is, indeed, possible to specify a number of different standards of conformity between the observations and the theoretical curve, which definitely lead to different though mutually approximate results. This mutual approximation, though convenient in practice in that it allows a computer to make a legitimate choice of the method which is arithmetically simplest, is harmful from the theoretical standpoint as tending to obscure the practical discrepancies, and the theoretical indefiniteness which actually exist.

2. Two methods of curve fitting may first be noted, in which we shall use a sign of summation when the observations comprise a finite number of ordinates only, and an integral sign when the curve itself is observed, even though the integrals may in practice be estimated by a process of summation.

Consider f a function of known form, involving arbitrary elements $\theta_1, \theta_2, \ldots, \theta_r$ and x the abscissa; let y be the observed ordinate corresponding to a given x. Then a natural method of getting suitable values for $\theta_1, \theta_2, \ldots, \theta_r$, that is of fitting the observations, is to make $\int_{-\infty}^{+\infty} (f-y)^2 dx$ a minimum for variations of any θ; or if the ordinate is observed at finite and equal intervals of the abscissa, we should substitute $\Sigma (f-y)^2$ for the integral.

This method will obviously give a good result to the eye in cases where a good result is possible; the equations to which it gives rise are, however, often practically insoluble, a difficulty which renders the method less useful than the simplicity of its principle would suggest.

The method of moments is possibly of more value, though its arbitrary nature is more apparent. If we solve the first r equations of the type

$$\int_{-\infty}^{+\infty} f\,dx = \int_{-\infty}^{+\infty} y\,dx \qquad \text{or } \Sigma f = \Sigma y,$$

$$\int_{-\infty}^{+\infty} xf\,dx = \int_{-\infty}^{+\infty} xy\,dx \qquad \text{or } \Sigma xf = \Sigma x,$$

$$\int_{-\infty}^{+\infty} x^2 f\,dx = \int_{-\infty}^{+\infty} x^2 y\,dx, \text{ etc. or } \Sigma x^2 f = \Sigma x^2 y, \text{ etc.},$$

we may obtain values for the r unknowns, which will give a curve to the eye about as good as that of least squares, by a method which for some purposes is found to be more convenient.

3. The first of the above methods is obviously inapplicable to frequency curves, even if we wished to accept its standard of "goodness of fit." If we suppose that the observations comprise a complete and continuous curve, an arbitrariness arises in the scaling of the abscissa line, for if ξ, any function of x, were substituted for x, the criterion would be modified. While, if a finite number of observations are grouped about a series of ordinates, there is an additional arbitrariness in choosing the positions of the ordinates and the distances between them.

For a finite number, n, of observations the method of moments really gives the equations

$$\Sigma f = n, \qquad \Sigma xf = \sum_1^n x, \qquad \Sigma x^2 f = \sum_1^n x^2, \qquad \text{etc.},$$

against which the above objections cannot be urged; still a choice has been made without theoretical justification in selecting this set of r equations of the general form

$$\Sigma x^p f = \sum_1^n x^p.$$

But we may solve the real problem directly.

If f is an ordinate of the theoretical curve of unit area, then $p = f\delta x$ is the chance of an observation falling within the range δx; and if

$$\log P' = \sum_1^n \log p,$$

then P' is proportional to the chance of a given set of observations occurring. The factors δx are independent of the theoretical curve, so the probability of any particular set of θ's is proportional to P, where

$$\log P = \sum_1^n \log f.$$

The most probable set of values for the θ's will make P a maximum.

If a continuous curve is observed—*e.g.*, the period during which a barometer is above any level during the year is a continuous function from which may be derived the relative frequency with which it stands at any height—we should use the expression

$$\log P = \int_{-\infty}^{\infty} y \log f \, dx.$$

4. For example, let us take the normal curve of frequency of errors

$$f = \frac{h}{\sqrt{\pi}} e^{-h^2(x-m)^2},$$

where h and m are to be determined to fit a set of n observations. Our criterion gives, neglecting a constant term,

$$\begin{aligned}\log P &= n \log h - h^2 \Sigma (x-m)^2 \\ &= n \log h - h^2 n (m - \bar{x})^2 - h^2 \Sigma (x - \bar{x})^2,\end{aligned}$$

where $n\bar{x} = \Sigma x$.

Differentiating with respect to m, we get

$$-2h^2 n (m - \bar{x}) = 0,$$

and with respect to h

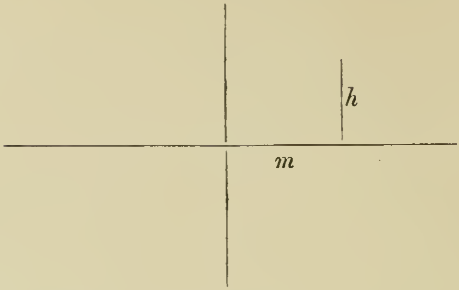
$$\frac{n}{h} = 2h \{n (m - \bar{x})^2 + \Sigma (x - \bar{x})^2\};$$

giving $m = \bar{x}$ $\qquad 2h^2 = \dfrac{n}{\Sigma v^2},$

where v is written for $x - \bar{x}$; neglecting the solution $h = 0$, $m = \infty$, when P is a minimum. Since the value usually accepted is

$$2h^2 = \frac{n-1}{\Sigma v^2},$$

it will be necessary to examine one or two of the methods by which this answer is obtained.



5. Corresponding to any pair of values, m and h, we can find the value of P, and the inverse probability system may be represented by the surface traced out by a point at a height P above the point on a plane, of which m and h are the coordinates.

The actual maximum of P occurs, as we have shown, at the point

$$m = \bar{x},$$

$$2h^2 = \frac{n}{\Sigma v^2}.$$

(a) In an interesting investigation* Mr. T. L. Bennett takes the maximum value of

$$\int_{-\infty}^{+\infty} P\,dm,$$

for variations of h, *i.e.*, of

$$h^n e^{-h^2 \Sigma (x-x)^2} \int_{-\infty}^{+\infty} e^{-h^2 n (m-\bar{x})^2}\,dm,$$

or of
$$\frac{\sqrt{\pi}}{h\sqrt{n}}\,h^n e^{-h^2 \Sigma v^2},$$

whence
$$(n-1)\,h^{n-2} = 2h^n \Sigma v^2$$

$$2h^2 = \frac{n-1}{\Sigma v^2},$$

a determination which gives the section perpendicular to the axis of h, the area of which is a maximum, though it does not pass through the actual maximum point.

* *Errors of Observation*, Technical Lecture, No. 4, 1907-08, Survey Department, Egypt.

We shall see (in § 6) that the integration with respect to m is illegitimate and has no definite meaning with respect to inverse probability.

(*b*) The usual text-book discussion* of the relation between h^2 and μ^2, where $n\mu^2 = \Sigma v^2$, assumes that the observed value of μ^2 is the same as the average value for a large number of sets of n observations each; thus the average value of $(x-m)^2$ being $\frac{1}{2h^2}$, the average value of $(\bar{x}-m)^2$—that is of

$$\frac{1}{n^2}(x_1 - m + x_2 - m \ldots x_n - m)^2$$

equals the average value of $\frac{1}{n^2}\overset{1}{\underset{n}{\Sigma}}(x-m)^2$, since the product terms go out—is

$$\frac{1}{n^2}\,\frac{n}{2h^2} = \frac{1}{2nh^2},$$

and the average value of $n\mu^2 = \Sigma(\bar{x}-x)^2$ is that of

$$\Sigma(m-x)^2 - n(\bar{x}-m)^2,$$

that is
$$\frac{n}{2h^2} - \frac{1}{2h^2} = \frac{n-1}{2h^2};$$

and if the most probable value for h was such as to make the observed quantity μ^2 take up its average value we should have

$$h^2 = \frac{n-1}{2n\mu^2}.$$

The basis of the above method becomes less convincing when we consider that the frequencies with which different values of μ^2 occur, for a given value of h, cannot give a normal distribution, since μ^2 can only vary from 0 to $+\infty$; and that a frequency distribution might easily be constructed to have a zero at its mean, in which case the above basis would give us perhaps the only value for h, which could not possibly have given rise to the observed value of μ^2.

The distinction between the most probable value of h, and the value which makes μ^2 take up its average value, is illustrated by our treatment of the quantity $(\bar{x}-m)^2$, the average value of which is $\frac{1}{2nh^2}$, but the most probable value being zero, we say that the most probable value of m is $\bar{x}$, not $\bar{x} \pm \frac{1}{h\sqrt{(2n)}}$.

* Chauvenet, *Spherical Astronomy*, Note II., Appendix § 17.

If a frequency curve of unit area were drawn, showing the frequencies with which different values of μ^2 occur, for a given h, and if b were the ordinate corresponding to the observed μ^2, then we should expect the equation

$$\frac{\partial b}{\partial h} = 0$$

to give the most probable value of h. It is sufficient here, however, to point out the incorrectness of the assumption upon which some writers on the Theory of Errors have based their results.

6. We have now obtained an absolute criterion for finding the relative probabilities of different sets of values for the elements of a probability system of known form. It would now seem natural to obtain an expression for the probability that the true values of the elements should lie within any given range. Unfortunately we cannot do so. The quantity P must be considered as the relative probability of the set of values $\theta_1, \theta_2, \ldots, \theta_r$; but it would be illegitimate to multiply this quantity by the variations $d\theta_1, d\theta_2, \ldots, d\theta_r$, and integrate through a region, and to compare the integral over this region with the integral over all possible values of the θ's. P is a relative probability only, suitable to compare point with point, but incapable of being interpreted as a probability distribution over a region, or of giving any estimate of absolute probability.

This may be easily seen, since the same frequency curve might equally be specified by any r independent functions of the θ's, say $\phi_1, \phi_2, \ldots, \phi_r$, and the relative values of P would be unchanged by such a transformation; but the probability that the true values lie within a region must be the same whether it is expressed in terms of θ or ϕ, so that we should have for all values $\frac{\partial(\theta_1, \theta_2, \ldots, \theta_r)}{\partial(\phi_1, \phi_2, \ldots, \phi_r)} = 1$ a condition which is manifestly not satisfied by the general transformation.

In conclusion I should like to acknowledge the great kindness of Mr. J. F. M. Stratton, to whose criticism and encouragement the present form of this note is due.

NOTE ON A CERTAIN FUNCTIONAL RECIPROCITY IN THE THEORY OF FOURIER SERIES.

By *W. H. Young, Sc.D., F.R.S.*

§ 1. The theory of the allied series of a Fourier series enables us to recognise without difficulty the existence of a remarkable reciprocity between two periodic functions of a real variable. I propose in the present note to call attention to certain problems in connection with it which await solution.

Denoting by $f(x)$ one of the functions, it may happen that

$$\frac{1}{\pi}\int_0^\infty \frac{f(x+t)-f(x-t)}{t}\,dt \quad\text{.................(1)}$$

exists as a Lebesgue integral. If we denote this function of x by $g(x)$, it may then happen that

$$\frac{1}{\pi}\int_0^\infty \frac{g(x+t)-g(x-t)}{t}\,dt \quad\text{.................(2)}$$

also exists as a Lebesgue integral. The reciprocity in question consists in the fact that if this latter integral does usually exist, its value is $f(x)$.

In fact, if (1) exists in the Lebesgue sense, the allied series of the Fourier series of $f(x)$, which we suppose summable, converges everywhere, and is accordingly a Fourier series, having $g(x)$ for sum, and therefore having $g(x)$ for the function of which it is the Fourier series. Since the allied series of the allied series is the original Fourier series, the reciprocity in question immediately follows.

We may evidently, if we please, substitute for the integrals (1) and (2) the expressions

$$\frac{1}{2\pi}\int_0^\pi \{f(x+t)-f(x-t)\}\cot\tfrac{1}{2}t\,dt \quad\text{..........(1')}$$

and
$$\frac{1}{2\pi}\int_0^\pi \{g(x+t)-g(x-t)\}\cot\tfrac{1}{2}t\,dt \quad\text{..........(2')}$$

without in any way altering the character of the reciprocity.

§ 2. If $f(x)$ is the integral of a function whose square is summable, $g(x)$ certainly exists and is a continuous function.

Moreover, since the Fourier series of $f'(x)$ is such that the sum of the squares of its coefficients converges, it follows that the same is true of the allied series of the Fourier series of $f'(x)$, whence this allied series is itself the Fourier series of a function whose square is summable. Thus, under these circumstances, $g(x)$ is itself the integral of a function whose square is summable. Accordingly the reciprocity holds good.

A direct proof, not employing the series of Fourier, of the fact that, if $f(x)$ is such a function, $g(x)$ is one also, is a desideratum. This is equivalent to proving that if $f(x)$ is any function which has its square summable.

$$\int_0^1 \{f(x+t)+f(x-t)\} \log t \, dt$$

is the integral of a function whose square is summable.

If, on the other hand, $f(x)$ has its p^{th} power summable where p has any value greater than unity, it would appear that a corresponding statement holds good. A direct proof that this is so is also desirable.*

§ 3. It is not, however, necessary that $f(x)$ should be an integral in order that $g(x)$ may exist, or even for the reciprocity to hold in its entirety. It follows, from some work of Fatou's,† that if $f(x)$ satisfies a condition of Lipschitz, $g(x)$ exists and also satisfies a condition of Lipschitz, so that the reciprocity holds. Now, though the integral of a function of which some power greater than the first is summable necessarily satisfies a condition of Lipschitz, the converse by no means always holds. If the index of the Lipschitz condition is unity, the function is certainly an integral, but there is nothing to indicate that this remains the case when the index is less than unity; indeed, to assert the contrary would imply that a function could not satisfy a condition of Lipschitz without having bounded variation.

Fatou's result is so far incomplete that it gives us no information as to the extent, if any, to which the condition of Lipschitz satisfied by $g(x)$ differs as regards index from that satisfied by $f(x)$. I propose, therefore, now to show that if we modify the condition of Lipschitz in the manner in

---

* F. Riesz has given a necessary and sufficient condition that a function should be the integral of a function whose $(1+p)$th power is summable. "Systeme integrierbarer Funktionen." *Math. Ann.*, vol. lxix., pp. 449–497. Other references bearing on the present article may be found in this paper.

† Fatou, "Sur les séries trig. et les séries de Taylor...," *Acta Mathematica*, xxx.

which I have already explained in a previous paper, so as to make it refer to a set of values of the index whose upper bound does not necessarily belong to the set, the condition satisfied by $g(x)$ is then the same as that satisfied by $f(x)$. It still remains, however, a subject of investigation as to whether the same statement is not true when the condition of Lipschitz is enunciated in the original form. This investigation would appear to be less difficult than that to which allusion is made in § 2. It should not be too difficult either to construct an example showing that this is not the case, or to so modify the reasoning as to prove the extension in question.

§ 4. THEOREM. *If for all values of h numerically less than a fixed quantity H, and for every positive value of a less than a fixed quantity $p \leq 1$, we have*

$$|f(u+h)-f(u)| < A\,|h|^a,$$

where A is a quantity, depending only on a, then, for all values of h less than a fixed quantity K,

$$|g(u+h)-g(u)| < B\,|h|^b,$$

B being a fixed quantity dependent in general on b, and b being any positive quantity less than p, where $g(u)$ is defined by the equation

$$2\pi . g(u) = \int_0^\pi \{f(u+t)-f(u-t)\} \cot \tfrac{1}{2}t\, dt.$$

Taking any positive value of $h < \frac{1}{2}H$, let us write

$$2\pi . g(u) = P_h(u) + Q_h(u) \ldots\ldots\ldots\ldots\ldots (1),$$

where $$Q_h(u) = \int_0^h \{f(u+t)-f(u-t)\} \cot \tfrac{1}{2}t\, dt \ldots\ldots (2),$$

and therefore

$$|Q_h(u)| \leq \int_0^h A\,(2t)^a \cot \tfrac{1}{2}t\, dt \leq \int_0^h A\,(2t)^{a-1}\, 4\, dt \leq 2A\,(2h)^a / a.$$

Hence $$|Q_h(u+h) - Q_h(u-h)| \leq 4A\,(2h)^a / a \ldots\ldots\ldots (3).$$

Again, by (1) and (2),

$$P_h = \int_h^\pi \{f(u+t) - f(u-t)\} \cot \tfrac{1}{2}t\, dt,$$

and therefore

$$|P_h(u+h)-P_h(u)|$$

$$= \left|\int_h^\pi \{f(u+t+h)-f(u+t)-f(u-t+h)+f(u-t)\}\cot\tfrac{1}{2}t\,dt\right|$$

$$\leq \left|\int_h^\pi 2A\,h^a\cot\tfrac{1}{2}t\,dt\right| \leq 4A\,h^a\,|\log\sin\tfrac{1}{2}h| \quad\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4).$$

Now, whatever positive fixed value be imputed to e,

$$\operatorname*{Lt}_{h=0} h^e\log\sin\tfrac{1}{2}h = 0.$$

Hence we can certainly find K, less than $\frac{1}{2}H$, and dependent on e, such that, for all values of $h<K$,

$$h^e\,|\log\sin\tfrac{1}{2}h|<1.$$

Thus, if the quantity e was chosen less than a, we shall have, by (4), for all values of $h<K$,

$$|P_h(u+h)-P_h(u)|<4A\,h^{a-e} \quad\ldots\ldots\ldots\ldots(5).$$

Hence, by (1), (3), and (5), for all values of $h<K$,

$$2\pi\,|g(u+h)-g(u)|<h^{a-e}A\,(4+2^{a+2}h^e/a)$$

$$<h^{a-e}A\,(4+8/a)<h^{a-e}A\,\{4+8/(a-e)\},$$

provided K is less than 1, and therefore h^e is less than unity.

Now, if b is any positive quantity less than p, we can find a greater than b and less than p, *e.g.*, $a=\frac{1}{2}(b+p)$. Denoting $(a-b)$ by e and $A(4+8/b)$ by B, we then have, for all values of h less than the quantity above denoted by K,

$$2\pi\,|g(u+h)-g(u)|<h^bB.$$

This proves the theorem.

It will be noticed that the quantity B depends upon b, but the quantity K does not.

§ 5. So far we have considered only the possibility of (1), (2), (1′), and (2′) existing as Lebesgue integrals. It may happen, however, that, for example,

$$g(x)=\operatorname*{Lt}_{e\to 0}\frac{1}{\pi}\int_e^\pi\{f(x+t)-f(x-t)\}\cot\tfrac{1}{2}t\,dt \quad\ldots(1'')$$

exists without

$$\int_0^\pi\{f(x+t)-f(x-t)\}\cot\tfrac{1}{2}t\,dt$$

existing as an absolutely convergent integral.

It appears that if $f(x)$ has bounded variation and is continuous, the existence of $(1'')$ is sufficient to ensure the convergence to $g(x)$, so defined, of the allied series of the Fourier series of $f(x)$. If it should then happen that $g(x)$ itself has bounded variation and is continuous, we are sure that, for a suitable sequence of e's at least,

$$\underset{e \to 0}{\mathrm{Lt}} \frac{1}{\pi} \int_e^{\pi} \{g(x+t) - g(x-t)\} \cot \tfrac{1}{2} t \, dt \text{........} (2'')$$

will exist and be equal to $f(x)$. In fact, the uniqueness of the limit $(2'')$ is the necessary and sufficient condition* that the allied series of the Fourier series of $g(x)$ may converge, and it of course does so, as it is the Fourier series of the continuous function of bounded variation $f(x)$.

A direct proof that, if $(1'')$ and $(2'')$ exist, and $f(x)$ and $g(x)$ have bounded variation, the reciprocity holds, is a desideratum.

More generally, the circumstances under which $g(x)$ is a function of bounded variation, if $f(x)$ is so, require investigation.

§ 6. It should be scarcely necessary to add that the problem suggested for solution is by no means the only one in this connexion which presents itself naturally, or that it breaks up into three well-defined parts of determining conditions sufficient, necessary, or necessary and sufficient for the existence of $g(x)$, for the existence of the corresponding integral involving $g(x)$, and of the determination of the nature of $g(x)$. Moreover, it is clear that we may extend the meaning of the word existence in a variety of ways. It may be well, however, to remark that we may replace the integral (1) by

$$\frac{1}{\pi} \frac{d}{dx} \int_0^{\infty} \frac{F(x+t) - F(x-t)}{t} dt,$$

where $F(x)$ is one of the indefinite integrals of $f(x)$, and that a similar modification may be made in the form of the integral (2).. This constitutes a generalisation of our point of view. If (1) exists, for example, the integral in the modified form just written down as a differential coefficient certainly exists, and the expression is usually equal to (1), while the contrary is by no means necessarily the case.

---

* See two papers by the author: one in the *Münchener Bericht*, 1911, "Zur Theorie des verwandten Reihe"; the other in *Proc. L.M.S.*, 1911, "On the nature of the succession formed by the Fourier constants of a function."

§ 7. I terminate this note by showing, in reference to the remark in § 3, that the well-known function of Weierstrass

$$f(x) = \sum_{n=0} b^n \cos(a^n x),$$

where a is an odd integer ≥ 7 and b a positive quantity less than unity, such that

$$ab > 1 + \tfrac{3}{2}\pi,$$

constructed by him as an example of a continuous function which at no point possesses a differential coefficient, and which accordingly is certainly not a function of bounded variation, although its Fourier series is uniformly convergent, does not satisfy any condition of Lipschitz. In fact, Weierstrass has shown* that

$$\left|\frac{f(x') - f(x_0)}{x' - x_0}\right| \geq (ab)^m . \left(\tfrac{2}{3} - \frac{\pi}{ab - 1}\right),$$

where the right-hand side is positive in virtue of the inequality satisfied by ab, x_0 being any point, and x' defined by the formula

$$x' - x_0 = -\frac{1 + x_{m+1}}{a^m},$$

where x_{m+1} lies between $-\frac{1}{2}$ and $\frac{1}{2}$. Hence

$$\frac{|f(x') - f(x_0)|}{|x' - x_0|^d} = |x' - x_0|^{1-d} \left|\frac{f(x') - f(x_0)}{x' - x_0}\right|$$

$$\geq a^{md} b^m (1 + x_{m+1})^{1-d} . \left(\tfrac{2}{3} - \frac{\pi}{ab - 1}\right) \geq a^{md} b^m 2^{d-1} \left\{\tfrac{2}{3} - \frac{\pi}{ab - 1}\right\}.$$

But, as m increases indefinitely, the right-hand side of this inequality, which is always positive, increases without limit, whatever positive value d may have. Thus $f(x)$ obeys no condition of Lipschitz.

---

* K. Weierstrass, "Zur Functionenlehre," 1880. *Monatsber. der k. Ak. d. Wiss. zu Berlin. Abh. aus d. Functionenlehre*, p. 99.

LAGRANGE'S DETERMINANTAL EQUATION IN THE CASE OF A CIRCULANT.

By *Thomas Muir, LL.D.*

1. If any circulant, $C(a, b, c, d)$ say, be taken in its standard form

$$\begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix},$$

that is to say, with the secondary diagonal as the axis of symmetry, and x be added to each diagonal element, the factors of the resulting determinant are of the same character as before, $a+x$ merely taking the place of a. The effect is quite different if the circulant be written in the alternative form

$$(-1)^{\frac{1}{2}(4-2)(4-1)}\begin{vmatrix} a & b & c & d \\ b & c & d & a \\ c & d & a & b \\ d & a & b & c \end{vmatrix} \quad \text{or } C'(a, b, c, d), \text{ say,}$$

where it is the *principal* diagonal that is the axis of symmetry. Attention was first drawn to this by Glaisher in the year 1877, and in a paper of the following year* he formulated the interesting theorem that *after removing from*

$$\begin{vmatrix} a_1+x & a_2 & a_3 & \cdots & a_n \\ a_2 & a_3+x & a_4 & \cdots & a_1 \\ a_3 & a_4 & a_5+x & \cdots & a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_n & a_1 & a_2 & \cdots & a_{n-1}+x \end{vmatrix}, \textit{ or } G_n(x) \textit{ say,}$$

the factor $\qquad x+(a_1+a_2+\ldots+a_n)$

* *Quart. Journal of Math.*, xv., pp. 347–356.

and also, if n *be even, the factor*

$$x + (a_1 - a_2 + \ldots - a_n)$$

there remains a series of quadratic factors of the form $x^2 - P$. The proof given by him is obtained by forming a set of linear equations having $G(x)$ for the visible eliminant, and then effecting elimination in such a way as to bring out a different form of result.

The main object of the present note is to throw additional light on this theorem.

2. If we take for shortness' sake the case where $n = 5$, we readily see that

$$\begin{vmatrix} a+x & b & c & d & e \\ b & c+x & d & e & a \\ c & d & e+x & a & b \\ d & e & a & b+x & c \\ e & a & b & c & d+x \end{vmatrix} \cdot \begin{vmatrix} a-x & b & c & d & e \\ b & c-x & d & e & a \\ c & d & e-x & a & b \\ d & e & a & b-x & c \\ e & a & b & c & d-x \end{vmatrix}$$

$$= \begin{vmatrix} A-x^2 & B & C & C & B \\ B & A-x^2 & B & C & C \\ C & B & A-x^2 & B & C \\ C & C & B & A-x^2 & B \\ B & C & C & B & A-x^2 \end{vmatrix},$$

where A stands for $(a, b, c, d, e \between a, b, c, d, e)$,

B ,, (,, $\between b, c, d, e, a)$,

C ,, (,, $\between c, d, e, a, b)$,

and where, be it observed, the resulting circulant is doubly axisymmetric.

By removing from the one side of this equality the factors

$$(a+b+c+d+e)+x, \qquad (a+b+c+d+e)-x,$$

and from the other side the corresponding factor

$$A + 2B + 2C - x^2,$$

i.e., $$(a+b+c+d+e)^2 - x^2,$$

there results the identity

$$\begin{vmatrix} 1 & b & c & d & e \\ 1 & c+x & d & e & a \\ 1 & d & e+x & a & b \\ 1 & e & a & b+x & c \\ 1 & a & b & c & d+x \end{vmatrix} \cdot \begin{vmatrix} 1 & b & c & d & e \\ 1 & c-x & d & e & a \\ 1 & d & e-x & a & b \\ 1 & e & a & b-x & c \\ 1 & a & b & c & d-x \end{vmatrix}$$

$$= \begin{vmatrix} 1 & B & C & C & B \\ 1 & A-x^2 & B & C & C \\ 1 & B & A-x^2 & B & C \\ 1 & C & B & A-x^2 & B \\ 1 & C & C & B & A-x^2 \end{vmatrix} .$$

But a determinant like that on the right* is known to be an exact square; and as we know at the same time that neither of the determinants on the left contains a square factor, it follows that the said two determinants are identical, and that therefore each is free of odd powers of x. Further, the form of the factors on the right being $(P-x^2)^2$, the form of the factors of each determinant on the left must be $P-x^2$, as was to be proved. (I.)

The procedure is quite similar when the order of the given circulant is even.

3. Not only, however, can the quotient of $G_5(x)$ by $a+b+\ldots+e+x$ be resolved as stated, but it can be expressed in a form analogous to that of $G(x)$ itself, namely, as an axisymmetric determinant with $-x^2$ as part of each diagonal element.

For example, the four factors of

$$C(A-x^2,\ B,\ C,\ C,\ B) \div (A+2B+2C-x^2)$$

being
$$\begin{aligned} &A-x^2+\epsilon B+\epsilon^2 C+\epsilon^3 C+\epsilon^4 B, \\ &A-x^2+\epsilon^2 B+\epsilon^4 C+\epsilon C+\epsilon^3 B, \\ &A-x^2+\epsilon^3 B+\epsilon C+\epsilon^4 C+\epsilon^2 B, \\ &A-x^2+\epsilon^4 B+\epsilon^3 C+\epsilon^2 C+\epsilon B, \end{aligned}$$

* Namely, a determinant originating as here from removal of the factor $a_1+2a_2+2a_3+\ldots$ from a odd-ordered circulant of the form

$$C'(a_1, a_2, a_3, a_4 \ldots, a_4, a_3, a_2).$$

See *Proceed. R. Soc. Edinburgh*, XXI., pp. 369–382, §§ 11–15

where ϵ is an imaginary fifth root of 1, we have, as above,

$$G_5(x) \div (a+b+c+d+e+x)$$
$$= (A-x^2+\epsilon B+\epsilon^2 C+\epsilon^3 C+\epsilon^4 B)(A-x^2+\epsilon^2 B+\epsilon^4 C+\epsilon C+\epsilon^3 B)$$
$$= x^4 - x^2\{2A + B(\epsilon+\epsilon^4+\epsilon^2+\epsilon^3) + C(\epsilon^2+\epsilon^3+\epsilon^4+\epsilon)\}$$
$$+ \{A + (\epsilon+\epsilon^4)B + (\epsilon^2+\epsilon^3)C\}\{A + (\epsilon^2+\epsilon^3)B + (\epsilon^4+\epsilon)C\},$$
$$= x^4 - x^2(2A-B-C) + (A^2-B^2-C^2-2AB-2AC+3BC)$$
$$= \begin{vmatrix} A-B-x^2 & B-C \\ B-C & A-C-x^2 \end{vmatrix}. \qquad \text{(II.)}$$

4. The general identity of which this is a case is dependent on an interesting proposition regarding an axisymmetric determinant whose elements are the $\frac{1}{2}n(n-1)$ differences of any n quantities.

The axisymmetric determinant which has the differences $a_1-a_2,\ a_1-a_3,\ \ldots,\ a_1-a_n$ *in the*

$$1^{\text{st}},\ n^{\text{th}},\ 2^{\text{nd}},\ (n-1)^{\text{th}},\ \ldots$$

places of the principal diagonal, the differences $a_2-a_3,\ a_2-a_4,\ \ldots,\ a_2-a_n$ *similarly disposed in the adjacent minor diagonal, the differences* $a_3-a_4,\ a_3-a_5,\ \ldots,\ a_3-a_n$ *similarly disposed in the next diagonal, and so on, is resolvable into linear factors, being equal to the* $n-1$ *different expressions of the form*

$$a_1 + (\omega+\omega^{2n-2})a_2 + (\omega^2+\omega^{2n-3})a_3 + \ldots + (\omega^{n-1}+\omega^n)a_n,$$

where ω *is an imaginary* $(2n-1)^{\text{th}}$ *root of* 1. (III.)

This is established by performing the operation

$$\text{col}_1 + (1+\theta_1)\,\text{col}_2 + (1+\theta_1+\theta_2)\,\text{col}_3 + \ldots,$$

where θ_r stands for $\omega^r + \omega^{2n-r-1}$.

For example, when $n=4$ and η is an imaginary 7^{th} root of 1, if we perform on the determinant

$$\begin{vmatrix} a_1-a_2 & a_2-a_3 & a_3-a_4 \\ a_2-a_3 & a_1-a_4 & a_2-a_4 \\ a_3-a_4 & a_2-a_4 & a_1-a_3 \end{vmatrix}$$

the operation

$$\text{col}_1 + (1+\eta+\eta^6)\,\text{col}_2 + (1+\eta+\eta^6+\eta^2+\eta^5)\,\text{col}_3,$$

the first column becomes

$$a_1 + (\eta+\eta^6)a_2 + (\eta^2+\eta^5)a_3 + (\eta^3+\eta^4)a_4,$$
$$(1+\eta+\eta^6)\{a_1 + (\eta+\eta^6)a_2 + (\eta^2+\eta^5)a_3 + (\eta^3+\eta^4)a_4\},$$
$$(1+\eta+\eta^6+\eta^2+\eta^5)\{a_1 + (\eta+\eta^6)a_2 + (\eta^2+\eta^5)a_3 + (\eta^3+\eta^4)a_4\},$$

and from the factor thus obtained it is seen that the determinant equals the product

$$\{a_1 + (\eta + \eta^6)\, a_2 + (\eta^2 + \eta^5)\, a_3 + (\eta^3 + \eta^4)\, a_4\}$$
$$\cdot\,\{a_1 + (\eta^2 + \eta^5)\, a_2 + (\eta^4 + \eta^3)\, a_3 + (\eta^6 + \eta)\, a_4\}$$
$$\cdot\,\{a_1 + (\eta^3 + \eta^4)\, a_2 + (\eta^6 + \eta)\, a_3 + (\eta^2 + \eta^5)\, a_4\}.$$

5. The next case of the theorem of § 3 thus is

$$\begin{vmatrix} a+x & b & c & \ldots & g \\ b & c+x & d & \ldots & a \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ g & a & b & \ldots & f+x \end{vmatrix}$$
$$= (x + a + \ldots + g) \begin{vmatrix} A - B - x^2 & B - C & C - D \\ B - C & A - D - x^2 & B - D \\ C - D & B - D & A - C - x^2 \end{vmatrix},$$

where A is the product of the first row of $G_7(0)$ by itself, B the product of the first and second rows, and so on. (II.′)

The two corresponding cases when n is even are

$$\begin{vmatrix} a+x & b & c & \ldots & f \\ b & c+x & d & \ldots & a \\ c & d & e+x & \ldots & b \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ f & a & b & \ldots & e+x \end{vmatrix}$$
$$= (x + a + b + \ldots + f)(x + a - b + c - d + e - f)$$
$$\cdot \begin{vmatrix} A - C - x^2 & B - D \\ B - D & A - C - x^2 \end{vmatrix},$$

$$\begin{vmatrix} a+x & b & c & \ldots & h \\ b & c+x & d & \ldots & a \\ c & d & e+x & \ldots & b \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ h & a & b & \ldots & g+x \end{vmatrix}$$
$$= (x + a + b + \ldots + h)(x + a - b + \ldots + g - h)$$
$$\cdot \begin{vmatrix} A - C - x^2 & B - D & C - E \\ B - D & A - E - x^2 & B - D \\ C - E & B - D & A - C - x^2 \end{vmatrix},$$

where A, B, ... are products of pairs of rows exactly as before, but where the law of formation of the determinant is somewhat diverse, no odd-numbered member of the series A, B, C, ... being subtracted from, or diminished by, an even-numbered member. (IV.)

6. In the cases where n is even the resulting determinant in x^2 is seen to be centrosymmetric, and therefore is resolvable into two determinants. Thus the two-line determinant factor of $G_6(x)$ in § 5 breaks up into

$$(A-C+B-D-x^2)\,(A-C-B+D-x^2),$$

and the corresponding factor of $G_8(x)$ into

$$(A-2C+E-x^2)\begin{vmatrix} A-E-x^2 & B-D \\ 2B-2D & A+E-x^2 \end{vmatrix}. \qquad \text{(V.)}$$

7. The fact that there are no odd powers of x in the development of an odd-ordered determinant like that in § 2 resulting from $G_5(x)$ by removal of the factor $a+b+c+d+e+x$ leads to a series of interesting identities, for example, in the said case of $n=5$, the identity

$$\begin{vmatrix} 1 & b & c & d \\ 1 & c & d & e \\ 1 & d & e & a \\ 1 & e & a & b \end{vmatrix} + \begin{vmatrix} 1 & b & c & e \\ 1 & c & d & a \\ 1 & d & e & b \\ 1 & a & b & d \end{vmatrix} + \begin{vmatrix} 1 & b & d & e \\ 1 & c & e & a \\ 1 & e & b & c \\ 1 & a & c & d \end{vmatrix} + \begin{vmatrix} 1 & c & d & e \\ 1 & e & a & b \\ 1 & a & b & c \\ 1 & b & c & d \end{vmatrix} = 0.$$

Towards proving this, the second and fourth determinants are transformed into

$$\begin{vmatrix} 1 & b & a & d \\ 1 & c & b & e \\ 1 & d & c & a \\ 1 & e & d & b \end{vmatrix}, \quad \begin{vmatrix} 1 & b & d & c \\ 1 & c & e & d \\ 1 & e & b & a \\ 1 & a & c & b \end{vmatrix},$$

We are thus enabled to see that the sum of the four is equal to

$$\begin{vmatrix} 1 & b & a+c & d \\ 1 & c & b+d & e \\ 1 & d & c+e & a \\ 1 & e & d+a & b \end{vmatrix} + \begin{vmatrix} 1 & b & d & c+e \\ 1 & c & e & d+a \\ 1 & e & b & a+c \\ 1 & a & c & b+d \end{vmatrix}.$$

In like fashion we next see the sum to be

$$= \begin{vmatrix} 1 & b & a+c & d \\ 1 & c & b+d & e \\ 1 & d & c+e & a \\ 1 & e & d+a & b \end{vmatrix} + \begin{vmatrix} 1 & b & a+c & e \\ 1 & c & b+d & a \\ 1 & d & c+e & b \\ 1 & e & d+a & c \end{vmatrix}$$

$$= \begin{vmatrix} 1 & b & a+c & d+e \\ 1 & c & b+d & e+a \\ 1 & d & c+e & a+b \\ 1 & e & d+a & b+c \end{vmatrix} = \begin{vmatrix} 1 & b & a+c & 1 \\ 1 & c & b+d & 1 \\ 1 & d & c+e & 1 \\ 1 & e & d+a & 1 \end{vmatrix} (a+b+c+d+e)$$

$$= 0.$$

The general theorem is that *if the elements of the first column of any odd-ordered circulant, axisymmetric with respect to the principal diagonal, be replaced by units, the sum of the complementary minors of the elements in the places* (2, 2), (3, 3), ..., (n, n) *vanishes*, or, say,

$$[2, 2] + [3, 3] + \ldots + [n, n] = 0. \qquad \text{(VI.)}$$

In the case where $n = 7$ not only does this hold, but we can substitute for it

$$[2, 2] + [3, 3] + [5, 5] = 0 = [4, 4] + [6, 6] + [7, 7],$$

the two zeros here originating in

$$\begin{vmatrix} 1 & c & d+a+b & e & f & g \\ 1 & e & f+c+d & g & a & b \\ 1 & f & g+d+e & a & b & c \\ 1 & g & a+e+f & b & c & d \\ 1 & a & b+f+g & c & d & e \\ 1 & b & c+g+a & d & e & f \end{vmatrix}, \quad \begin{vmatrix} 1 & b+f+a & c & d & e & g \\ 1 & c+g+b & d & e & f & a \\ 1 & d+a+c & e & f & g & b \\ 1 & e+b+d & f & g & a & c \\ 1 & f+c+e & g & a & b & d \\ 1 & a+e+g & b & c & d & f \end{vmatrix}.$$

8. A procedure similar to the foregoing enables us to complete a theorem of Stern's (*Crelle's Journal*, lxxiii., pp. 374–380) regarding the difference between the signed complementary minors of any two elements of a circulant.

Taking, to start with, any determinant whatever, $|a_1 b_2 c_3 d_4|$ say, we have

$$A_1 - A_2 = \begin{vmatrix} b_2 & b_3 & b_4 \\ c_2 & c_3 & c_4 \\ d_2 & d_3 & d_4 \end{vmatrix} + \begin{vmatrix} b_1 & b_3 & b_4 \\ c_1 & c_3 & c_4 \\ d_1 & d_3 & d_4 \end{vmatrix}$$

$$= \begin{vmatrix} b_1 + b_2 & b_3 & b_4 \\ c_1 + c_2 & c_3 & c_4 \\ d_1 + d_2 & d_3 & d_4 \end{vmatrix} = \begin{vmatrix} \Sigma b & b_3 & b_4 \\ \Sigma c & c_3 & c_4 \\ \Sigma d & d_3 & d_4 \end{vmatrix},$$

from which it appears that if $\Sigma b = \Sigma c = \Sigma d$, as is the case in a circulant, the common sum is a factor of $A_1 - A_2$. the co-factor being

$$\begin{vmatrix} 1 & b_3 & b_4 \\ 1 & c_3 & c_4 \\ 1 & d_3 & d_4 \end{vmatrix}.$$

The completed theorem referred to is that *if* $\mathrm{A}_1, \mathrm{A}_2, \ldots$ *be the signed complementary minors of* $\mathrm{a}_1, \mathrm{a}_2, \ldots$ *in the circulant* $\mathrm{C}(\mathrm{a}_1, \mathrm{a}_2, \ldots)$, *then*

$$\mathrm{A}_r - \mathrm{A}_s = (-1)^{r+s-1} (\mathrm{a}_1 + \mathrm{a}_2 + \ldots)\,\mathrm{Q},$$

where Q *is the determinant got from* C *by deleting the first row and the* r^{th} *and* s^{th} *columns and inserting a column of units in the first place.* (VII.)

Capetown, S.A.,
October 2nd, 1911.

SOME PROPERTIES OF THE INNER CONTENT FUNCTION.

By *A. R. Richardson*, University College, London, and Royal College of Science, London.

In what follows we consider the inner content of a set between the points 0 and x as a function of x. If Q denotes the set, $IQ(x)$ denotes the inner content of this set up to the point x. We prove that, in general, $\dfrac{IQ(x)}{x}$ has an infinite number of maxima and minima.

I. *If* $IQ(x)=f(x)\,IP(x)$ *and if in any interval* (c, d) $f(x)$ *never increases but is finite and continuous, then the points of* Q, *inside the interval, which do not belong to* P *have zero inner content.*

For, by definition of the inner content (Young's *Theory of Sets of Points*, p. 96), any set P may be regarded as made up of a closed set Pc, together with a set of inner content as small as we please.

Consider the interval $(0, b)$ and let

$$IP(b) = IPc(b) + \epsilon,$$

then, if x be any point inside this interval,

$$IP(x) = IPc(x) + \epsilon',$$

where $\epsilon' < \epsilon$.

Now Pc defines a complementary set of non-overlapping intervals δ_ν. Let (x_{ν_1}, x_{ν_2}) be the end points of such an interval δ_ν. Then no points of Pc lie inside or at the end points of such an interval. Therefore

$$\Sigma IP(\delta_\nu) \leqq \epsilon,$$

where $IP(\delta_\nu)$ is equal to the inner content of the points of P inside the interval δ_ν.

Now $\quad IQ(\delta_\nu) = f(x_{\nu_2})\,IP(x_{\nu_2}) - f(x_{\nu_1})\,IP(x_{\nu_1}).$

Suppose that in any interval (c, d) $f(x)$ never increases. Therefore

$$\begin{aligned} IQ(\delta_\nu) &\leqq f(x_{\nu_1})\left[IP(x_{\nu_2}) - IP(x_{\nu_1})\right] \\ &\leqq f(x_{\nu_1})\,IP(\delta_\nu), \end{aligned}$$

[if δ_ν be an interval inside (c, d), or if M be the upper limit of $f(x_\nu)$]

$$\leqq MIP(\delta_\nu).$$

Therefore summing for all δ_ν inside (c, d)

$$\begin{aligned} \Sigma IQ(\delta_\nu) &\leqq M\,\Sigma IP(\delta_\nu) \\ &\leqq M\epsilon \\ &< \epsilon''. \end{aligned}$$

Hence all points of Q, which lie inside these intervals, have content $< \epsilon''$. But all points of Q, which do not lie inside these intervals, belong to Pc. Therefore the inner content of those points of Q, inside (c, d), which do not belong to Pc, is $< \epsilon''$.

Take now $$\epsilon_1 > \epsilon_2 > \epsilon_3 \ldots > \epsilon_n \to 0,$$

and let $$Pc_1 < Pc_2 < Pc_3 \ldots < Pc_n \to P\omega,$$

where, by definition of inner content,

$$IP\omega(x) = IP(x).$$

Then, since Pc_n is a part of $P\omega$, the points of Q, inside (c, d), which do not belong to $P\omega$, have content $\leq \epsilon_n$. Therefore the points of Q, inside (c, d), which do not belong to $P\omega$, have zero inner content.

Incidentally we remark that similar reasoning will prove the converse of the well-known result that if

$$R(x) = P(x) + Q(x),$$

and $P(x)$ and $Q(x)$ have no common points and one is additive, then

$$IR(x) = IP(x) + IQ(x).$$

The result is that if $IR(x) = IP(x) + IQ(x)$, then the points of $P(x)$ and $Q(x)$ which do not belong to $R(x)$, and the points of $R(x)$ which belong to neither $P(x)$ nor $Q(x)$, have each zero inner content.

We now proceed to examine the character of $f(x)$. In doing so we may suppose $P(x)$ and $Q(x)$ to be additive, for in any set we can find an inner additive set having the same inner content as the set. Thus $f(x)$ will remain unaltered.

The following cases may arise:—

I. *The points of Q which do not belong to P have not zero inner content, and the points of P which do not belong to Q have not zero inner content.*

In this case, whether $P(x)$ and $Q(x)$ be additive or not, $f(x)$ cannot be monotone. This will still be the case over any sub-interval.

II. *The points of Q which do not belong to P have zero inner content, and the points of P which do not belong to Q have not zero inner content.*

Let $\xi(x)$ denote the points of $Q(x)$ which do not belong to $P(x)$. Let $P'(x) = P(x) + \xi(x)$ so that $P'(x)$ may be non-additive. $P(x)$ is however additive. Therefore

$$IP'(x) = IP(x),$$

since $$I\xi(x) = 0.$$

Therefore $$IQ(x) = f(x)\, IP'(x),$$

and now $Q(x)$ is a part of $P'(x)$, and the points of $P'(x)$, which do not belong to $Q(x)$, say $D(x)$, have not zero inner content, being the points of $P(x)$ which do not belong to $Q(x)$.

$$IP'(x) = IQ(x) + ID(x),$$

since Q is additive and $Q(x)$ and $D(x)$ have no common points. Therefore

$$IQ(x) = f(x)\, IQ(x) + f(x)\, ID(x).$$

Therefore $$ID(x) = \left\{\frac{1-f(x)}{f(x)}\right\} IQ(x),$$

but no point of $D(x)$ belongs to $Q(x)$ and neither is of zero inner content. Therefore $\frac{1-f(x)}{f(x)}$ cannot be monotone by I. Therefore $f(x)$ cannot be monotone. Hence, if in any interval, the content of the points of $D(x)$, inside this interval, are not zero, and the content of the points of $Q(x)$ are not zero, the $nf(x)$ cannot be monotone inside the interval.

A special case of this result is that in which $P(x)$ is the continuum, *i.e.*, $IP(x) = x$. Our result is then that $\frac{IQ(x)}{x}$ cannot be monotone in any interval unless inside that interval $Q(x)$ has either zero inner content or content equal to that of the continuum, *i.e.*, $\frac{IQ(x)}{x}$ will have, in general, an infinite number of maxima and minima.

In particular, no set exists which is homogeneous with respect to the content, *i.e.*, which is such that the content in all intervals of the same length is the same, except a set of zero inner content or of content equal to that of the continuum. For we should have

$$\phi(x+h) - \phi(x) - \phi(x-h)$$

for all x's and all h's. Therefore

$$\begin{aligned}\phi(x) &= \text{linear function of } x \\ &= kx, \text{ say, since } \phi(0) = 0,\end{aligned}$$

i.e., $$\frac{\phi(x)}{x} = \text{constant},$$

which we have just seen to be impossible.

III. *The points of one which do not belong to the other have zero inner content.*

In this case, referring to case II., $ID(x)=0$ for all x's, therefore $f(x)=1$.

Example to illlustrate that $\dfrac{IQ(x)}{x}$ *has an infinite number of maxima and minima:—*

Let $Q(x)$ be the set common to the black intervals of the example, Young's *Theory of Sets of Points*, p. 78. We divide the interval (0, 1) into three equal parts and blacken the central part. Each of the unblackened pieces are divided into 3^2 parts and the central part blackened, and each unblackened piece into 3^3 pieces, and so on.

Let x_{n+1}, x_n be the right- and left-hand end points respectively of one of these black intervals δ_n. Then

$$\frac{IQ(x_{n+1})}{x_{n+1}} \geqq \frac{IQ(x_n)}{x_n},$$

for

$$x_{n+1} = x_n + \delta_n$$

$$IQ(x_{n+1}) = IQ(x_n) + \delta_n,$$

and

$$x_n \geqq IQ(x_n).$$

Now let b denote the left-hand end point of any black interval at the n^{th} stage; ρ_{n+1} be the right-hand end point of the black interval at the $(n+1)^{\text{th}}$ stage, which is nearest to b. Let $b = \rho_{n+1} + \delta_{n+1}$, then

$I(b) = I(\rho_{n+1})$ + inner content of the set of black intervals which fall between b and ρ_{n+1}.

Now these intervals will have content as follows: at $(n+2)^{\text{th}}$ stage

$$\text{content} = \frac{\delta_{n+1}}{3^{n+2}},$$

at $(n+3)^{\text{rd}}$ stage

$$= \delta_{n+1}\left(1 - \frac{1}{3^{n+2}}\right)\frac{1}{3^{n+3}},$$

and so on. Therefore

$$\text{content of black intervals between } b \text{ and } \rho_{n+1}$$

$$= \frac{\delta_{n+1}}{3^{n+2}} + \delta_{n+1}\left(1 - \frac{1}{3^{n+2}}\right)\frac{1}{3^{n+3}}$$

$$+ \delta_{n+1}\left(1 - \frac{1}{3^{n+2}}\right)\left(1 - \frac{1}{3^{n+3}}\right)\frac{1}{3^{n+4}} + \dots$$

$$= \delta_{n+1}\left[1 - \prod_{s=2}^{s=\infty}\left(1 - \frac{1}{3^{n+s}}\right)\right].$$

Therefore
$$\frac{I(b)}{b} = \frac{I(\rho_{n+1}) + \delta_{n-1}\left[1 - \prod_{s=2}^{\infty}\left(1 - \frac{1}{3^{n+s}}\right)\right]}{\rho_{n+1} + \delta_{n+1}}$$
$$\gtreqless \frac{I(\rho_{n+1})}{\rho_{n+1}},$$

according as

$$\rho_{n+1} I(\rho_{n+1}) + \delta_{n+1}\rho_{n+1}\left[1 - \prod_{s=2}^{\infty}\left(1 - \frac{1}{3^{n+s}}\right)\right]$$
$$\gtreqless \rho_{n+1} I(\rho_{n+1}) + \delta_{n+1} I(\rho_{n+1}),$$

i.e., as
$$\rho_{n+1}\left[1 - \prod_{s=2}^{\infty}\left(1 - \frac{1}{3^{n+s}}\right)\right] \gtreqless I(\rho_{n+1}).$$

Now $\rho_{n+1} < b$, therefore the left-hand side is

$$< b\left[1 - \prod_{s=2}^{\infty}\left(1 - \frac{1}{3^{n+s}}\right)\right],$$

but
$$\prod_{s=2}^{\infty}\left(1 - \frac{1}{3^{n+s}}\right) > 1 - \frac{1}{3^{n+2}} - \frac{1}{3^{n+3}} + \ldots > 1 - \frac{1}{3^{n+2}} \cdot \frac{2}{3},$$

therefore the left-hand side is

$$< b \cdot \frac{2}{3^{n+3}}.$$

Now b is fixed so that by taking n large enough we may make the left-hand side as small as we please, and therefore $< I(\rho_{n+1})$, which must increase with n; therefore

$$\frac{I(b)}{b} < \frac{I(\rho_{n+1})}{\rho_{n+1}}.$$

Hence, in any interval, however small, which does not wholly belong to the set Q, $\frac{IQ(x)}{x}$ has an infinite number of maxima and minima, since, if b be a left-hand end point of a black interval, values of $\frac{IQ(x)}{x}$ can be found where x is as close to b as we please, of which some are $> \frac{I(b)}{b}$ and some $< \frac{I(b)}{b}$.

In conclusion my best thanks are due to Dr. L. N. G. Filon for his kind help.

NOTES ON INTEGRAL EQUATIONS.

By *H. Bateman.*

VIII.

Some simple definite integrals derived from the formulæ of Fourier and Abel.

1. THE work given on pp. 99 and 100 of my last note* is not quite complete. A factor $2/\pi$ has been omitted from some of the integrals and no mention was made of the restrictions laid upon $\phi(z)$. It is convenient to consider a function such that

$$\int_0^k |\phi(z)|\, dz$$

is convergent; with the aid of this restriction the change in the order of integration is easily justified.

A word or two of explanation is also necessary for the example on p. 100. It is implied that the equation

$$\int_0^\infty J_0(zt)\, dt \int_0^1 \sin xt . \cos^{-1} x\, dx = \int_z^1 \frac{\cos^{-1} x\, dx}{\sqrt{(x^2 - z^2)}}$$

$$= -\tfrac{1}{2}\pi \log z \quad (0 < z < 1)$$

may be justified by putting

$$J_0(zt) = \frac{2}{\pi} \int_z^\infty \frac{\sin tu}{\sqrt{(u^2 - z^2)}}\, du.$$

Making this substitution and evaluating the integral with regard to x, we have to justify a change in the order of integration in the repeated integral

$$\int_0^\infty [1 - J_0(t)] \frac{dt}{t^2} \int_z^\infty \frac{t \sin tu}{\sqrt{(u^2 - z^2)}}\, du.$$

The theorems given by Hardy in a recent note† do not seem to be applicable to this case because $[1 - J_0(t)]\, t^{-1}$ is not integrable in the infinite interval, but the change in the order of integration may be justified as follows.

By the analogue of Abel's lemma‡ we can choose m so that

$$\left| \int_m^\infty \frac{t \sin tu\, du}{\sqrt{(u^2 - z^2)}} \right| < \frac{2}{\sqrt{(m^2 - z^2)}} < \epsilon,$$

---

* Vol. XLI., pp. 94–101.

† Vol. XLI., p. 102.

‡ Bromwich, *Infinite Series*, p. 426.

where m and ϵ are independent of t; we have then

$$\left|\int_0^\infty \int_m^\infty\right| < \epsilon \int_0^\infty [1 - J_0(t)] \frac{dt}{t^2} < \epsilon K, \text{ say},$$

for $1 - J_0(t)$ is never negative.

Again, since the integral

$$\int_0^\infty \sin tu [1 - J_0(t)] \frac{dt}{t} = \cos^{-1} u \quad (0 < u < 1)$$
$$= 0 \quad (u > 1)$$

is uniformly convergent for $u \geq z > 0$, we may change the order of integration in the repeated integral $\int_0^\infty \int_z^m$ and obtain

$$\int_0^\infty \int_z^m = \int_z^m \int_0^\infty.$$

Lastly $\int_m^\infty \int_0^\infty = 0$, if $m > 1$, and so we have the inequality

$$\left|\int^\infty \int_0^\infty - \int_0^\infty \int_z^\infty\right| < \epsilon K.$$

Since ϵ is an arbitrary small quantity, the two repeated integrals must be equal.

2. If, in the equation

$$\int_0^\infty J_0(zt) \{1 - J_0(t)\} \frac{dt}{t} = -\log z \quad (z < 1)$$
$$= 0 \quad (z > 1),$$

we replace $J_0(zt)$ by the definite integral

$$\frac{2}{\pi} \int_0^z \frac{\cos ut}{\sqrt{(z^2 - u^2)}} du,$$

we obtain the equation

$$\int_0^\infty [1 - J_0(t)] \frac{dt}{t} \int_0^z \frac{\cos ut}{\sqrt{(z^2 - u^2)}} du = -\tfrac{1}{2}\pi \log z \quad (0 < z < 1)$$
$$= 0 \quad (z > 1).$$

A change in the order of integration is easily justified by a slight alteration of the previous method, and so we have the equation

$$(1) \qquad \int_0^z \frac{\phi(u)\, du}{\sqrt{(z^2 - u^2)}} = -\tfrac{1}{2}\pi \log z \quad (0 < z < 1)$$
$$= 0 \quad (z > 1),$$

where $$\int_0^\infty \cos ut [1 - J_0(t)] \frac{dt}{t} = \phi(u).$$

We shall now show that*

$$\phi(u) = -\log 2u \qquad (u \leq 1)$$

$$= -\log \frac{2u}{u + \sqrt{(u^2 - 1)}} \qquad (u \geq 1).$$

In the first place we have to show that

$$\log z = \frac{2}{\pi} \int_0^z \frac{\log 2u \, du}{\sqrt{(z^2 - u^2)}}.$$

This may be done by putting $u = z \sin\theta$, when the integral becomes

$$\frac{2}{\pi} \int_0^{\frac{1}{2}\pi} \log(2z \sin\theta)\, d\theta,$$

and the result follows at once from the known formula

$$\int_0^{\frac{1}{2}\pi} \log(\sin\theta)\, d\theta = -\tfrac{1}{2}\pi \log 2.$$

We have next to show that

$$\int_0^z \frac{\log 2u}{\sqrt{(z^2 - u^2)}}\, du = \int_1^z \frac{\log[u + \sqrt{(u^2 - 1)}]}{\sqrt{(z^2 - u^2)}}\, du,$$

or that

$$\log z = \frac{2}{\pi} \int_1^z \frac{\cosh^{-1} u \, du}{\sqrt{(z^2 - u^2)}}.$$

This may be done by means of Abel's inversion formula jus as in the case of the analogous integral in the last note,† for i

$$\log z = \frac{2}{\pi} \int_1^z \frac{\psi(u)\, du}{\sqrt{(z^2 - u^2)}},$$

the inversion formula gives

$$\psi(u) = \frac{d}{du} \int_1^u \frac{z \log z \, dz}{\sqrt{(u^2 - z^2)}}$$

$$= \frac{d}{du} \int_1^u \sqrt{(u^2 - z^2)}\, \frac{dz}{z}$$

$$= \int_1^u \frac{u\, dz}{z\sqrt{(u^2 - z^2)}} = -\left[\operatorname{sech}^{-1} \frac{z}{u}\right]_1^u$$

$$= \cosh^{-1} u.$$

---

* This value of $\phi(u)$ may also be deduced from the known integral

$$\int_0^\infty e^{-zt}[1 - J_0(t)]\, \frac{dt}{t} = -\log \frac{2z}{z + \sqrt{(1 + z^2)}} \qquad (z > 0).$$

† These integrals may be reduced to known forms by simple transformations.

Writing equation (1) in the standard form

$$\log x = \frac{1}{\pi}\int_0^x \frac{\log(4t)}{\sqrt{(x-t)}}\frac{dt}{\sqrt{t}},$$

we have a case in which Abel's equation

$$f(x) = \int_0^x \frac{\chi(t)\,dt}{\sqrt{(x-t)}}$$

is soluble when $f(x) \to \infty$ as $x \to 0$. It is easy to verify that the inversion formulæ

$$\chi(t) = \frac{1}{\pi}\frac{d}{dt}\int_0^t \frac{f(x)}{\sqrt{(t-x)}}\,dx$$

is applicable in this case* because

$$\int_0^t \frac{\log x}{\sqrt{(t-x)}}\,dx = 2\sqrt{t}\int_0^{\frac{1}{2}\pi}\log(t\sin^2\theta)\sin\theta\,d\theta$$

$$= 2\sqrt{t}\left[\log 4t - 2\right].$$

The analysis given in Bôcher's *Introduction to the study of Integral Equations* is applicable to this case if we define $f(x)$ to be zero when $x = 0$.

§3. Pringsheim states in a recent article (*Math. Ann.*, Bd. 68, 1910) that H. Weber has verified Fourier's formula for the case of the function $\frac{\sin x}{x}$. This means that, since

$$(1) \qquad \int_0^\infty \sin xz \,.\, \sin az\,\frac{dz}{z} = \tfrac{1}{2}\log\frac{x+a}{|x-a|},$$

we have

$$(2) \qquad \sin az = \frac{z}{\pi}\int_0^\infty \log\frac{a+x}{|a-x|}\sin xz\,dx \quad (z > 0).$$

The singular integral equation

$$\phi(a) = \lambda\int_0^\infty \log\frac{a+x}{|a-x|}\,\phi(x)\,dx$$

can thus be satisfied for all positive values of λ, and so the kernel $\log\frac{a+x}{|a-x|}$ possesses a band spectrum.

The integral (1) is well known,† for it may be evaluated

* H. W. March has considered the case in which $\chi(t)$ becomes infinite like $t^{-\lambda}$ $(0 < \lambda < 1)$ at $t = 0$. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, Bd. 20 (1911), p. 355. The well-known formula for the Beta function of course indicates that the inversion formula holds in a particular case of this kind.

† See, for instance, Schafheitlin, *Math. Ann.*, Bd. 30 (1887).

at once by Frullani's theorem. The integral (2) may be evaluated by regarding it as the limit, when $\epsilon \rightarrow 0$, of

$$\int_0^{a-\epsilon} + \int_{a-\epsilon}^{\infty}.$$

Integrating each integral by parts and making a change of variables the above value is easily obtained by making $\epsilon \rightarrow 0$.

The formula (2) indicates that in many cases the integral equation

$$f(x) = \frac{1}{\pi}\int_0^{\infty} \log \frac{a+x}{|a-x|}\,\phi(x)\,dx \quad (a>0) \ldots\ldots(3)$$

may be solved by means of the formula

$$\phi(x) = \int_0^{\infty} \sin xz \,.\, \chi(z)\,dz,$$

where $\chi(z)$ is determined from the equation

$$f(a) = \int_0^{\infty} \sin az \,.\, \chi(z)\frac{dz}{z}.$$

The following examples will illustrate this:

$$\int_0^{\infty} \log \frac{a+x}{|a-x|}\,\frac{x\,dx}{u^2+x^2} = \pi \tan^{-1}\frac{a}{u},$$

$$\int_0^{\infty} \log \frac{a+x}{|a-x|}\,\log \frac{b+x}{|b-x|}\,dx = \pi^2 a \quad (a<b)$$
$$= \pi^2 b \quad (a>b),$$

$$\int_u^{\infty} \log \frac{a+x}{|a-x|}\,\frac{dx}{\sqrt{(x^2-u^2)}} = \pi \sin^{-1}\frac{a}{u} \quad (0 \leq a < u)$$
$$= \tfrac{1}{2}\pi^2 \quad (a>u).$$

Formula (1) indicates that the kernel $\log \frac{x+a}{|x-a|}$ is definite for functions $\phi(x)$ such that $\int_0^{\infty} |\phi(x)|\,dx$ is convergent, and that consequently the solution of (3) is unique provided $\phi(x)$ is restricted in this way.

We cannot say at present that the solution is always unique, for if $\kappa(a, x)$ is a definite function for a limited class of functions, it is not known whether a function $\chi(x)$ not belonging to the class can satisfy the equation

$$0 = \int_0^{\infty} \kappa(a, x)\,\chi(x)\,dx \quad (a>0).$$

A PROBLEM IN CONGRUENCES.

By *T. C. Lewis, M.A.*, Trinity College, Cambridge.

§ 1. In each of the following arrangements the numbers are all multiples of 7, or give the same remainder on division by 7; also the sum of the pair of figures in each vertical column is constant. A set may begin with any number:

49	38	21
35	45	$5\bar{1}$
56	24	$6\bar{4}$
14	66	$4\bar{5}$
28	52	$1\bar{3}$
07	03	00

The numbers repeat after the first six if the series be continued in the same way. The final or sixth number of the period has a zero or a multiple of 7 in each place, with the constant remainder of the series added in its proper place if there is such remainder.

It is a remarkable fact that the numbers made up of each left-hand or right-hand set of figures, taken in reverse order, *i.e.*, from right to left, but written down from left to right, are all divisible by 7; *e.g.*, in the first set,

435120 and 956487.

Also, either set of alternate figures in any of these numbers may be replaced by zero, or by any number we please, or may be increased or decreased equally throughout, without affecting the divisibility by 7, as in the following numbers:

(i) replacing alternate figures by zero,

405020, 30100;

(ii) replacing by a constant number,

435323, 434140;

(iii) increasing by constant number,

445221, 536130.

The same is true whatever multiple of ten is taken out of the initial number to put into the tens' place, the positive or negative remainder taking the units' place. For instance,

the first of the above sets may be written variously as follows:

$$\begin{array}{lllllllllll}
 & & & & & 3.19 & & & & & 5.\bar{1} \\
 & & & & 4.16 & & & & & 2.\bar{6} & \\
 & & & 2.15 & & & & & 1.\bar{3} & & \\
 & & 6.17 & & & & & 3.\bar{2} & & & \\
 & 5.13 & & & & & 6.\bar{4} & & & & \\
0.14 & & & & & 0.\bar{7} & & & & &
\end{array}$$

and the properties indicated are still true.

In addition, the 1st and 4th figures may be increased by one number, the 2nd and 5th by another, and the 3rd and 6th by a third number without destroying the relation. Moreover, the two figures that make up any number of a set, or the three figures, as in the first of the last two cases, may be multiplied respectively by any three numbers (positive or negative) and added together; and in all cases the stated property remains unaffected.

These facts lead to the following general investigation.

§ 2. Let p be any number prime to r, and f the exponent to which r appertains (mod p), so that

$$r^f \equiv 1 \pmod{p}.$$

Then f is a factor of $\phi(p)$, the number of integers less than p and prime to it; it is also the number of "decimal" places that recur in the expression of $1/p$ in the scale of notation r.

Let m be the reciprocal of r (mod p), so that

$$rm \equiv 1 \pmod{p}.$$

In the following scheme of numbers, or equimultiples of them

$$\begin{array}{llll}
 & & -m, & 1, \\
 & -m^2-m, & m+1, & \\
-m^3-m^2-m, & m^2+m+1, & & \\
\ldots\ldots,\quad m^3+m^2+m+1, & & &
\end{array}$$

and so on, the left-hand numbers are $-m$ times those on the right, the sum of any vertical pair is a constant, and in any line the two-figured number in the scale of r is a multiple of p.

The right-hand set may be written

$$\frac{m-1}{m-1},\quad \frac{m^2-1}{m-1},\quad \frac{m^3-1}{m-1},\quad \ldots,\quad \frac{m^f-1}{m-1},\quad \&c.,$$

where $\dfrac{m^f-1}{m-1}$ is congruent with zero (mod p), unless $f=1$; or $m \equiv 1 \pmod{q}$, where q is a factor of p, but not of f. Thus, for the congruence with zero (mod p) to hold necessarily, either p must be prime to $m-1$, or their common factor must also be a factor of f. Let p be limited to these cases.

The number in the scale of r consisting of the first n figures, being

$$\frac{1}{m-1}\{r^{n-1}(m-1)+r^{n-2}(m^2-1)+\ldots+(m^n-1)\} \ldots (A),$$

becomes, when $n=f$,

$$\frac{1}{m-1}\{r^{f-1}(m-1)+r^{f-2}(m^2-1)+\ldots+(m^f-1)\} \ldots\ldots (B)$$

$$\equiv \frac{1}{m-1}\{m(m-1)+m^2(m^2-1)+\ldots+m^f(m^f-1)\}$$

$$(\text{since } r^n \equiv m^{f-n})$$

$$\equiv \frac{1}{m-1}\left\{m^2 . \frac{m^{2f}-1}{m^2-1} - m . \frac{m^f-1}{m-1}\right\}$$

$$\equiv 0 \pmod{p},$$

unless $f=1$ or 2; or $m \equiv 1 \pmod{q}$ or $m^2 \equiv 1 \pmod{q}$, where q is a factor of p but not of f. Thus, for the congruence to hold good, $f>2$ and p is either prime to $m-1$ and m^2-1, or the factor which it has in common with either must also be a factor of f. In this statement, $r-1$ and r^2-1 may be written in place of $m-1$ and m^2-1. If $f=1$, the residue is 1; if $f=2$, the residue is the same as of $2m+1$, which, when p is a prime, is $p-1$.

Since the successive f^{th} terms are congruent with zero, the congruence for the sum will hold for $f-1$ terms, and for nf and $nf-1$ terms.

It follows that in the scale of 10 the property holds good in general, *i.e.*, for all equimultipliers that may be employed in the original scheme, in the case of any number p which is prime to 10, with the following exceptions:

(i) those for which $f=1$ or 2, viz., 3, 9; 11, 33, 99;

(ii) those for which $m-1$ and p have a factor not contained in f, *e.g.*, 27, 51, 69, 87, 117, 123, 141, 153, 159, 177;

(iii) those other values for which m^2-1 and p have a factor not in f, *e.g.*, 77, 187.

The above values include all the exceptions up to 200.

In all cases where the sum of f terms is not congruent with zero $(\text{mod}\, p)$ the sum of certain multiples of f terms exhibits that congruence.

Any left-hand member in the scheme of numbers may be increased or diminished by any multiple of p if the number beneath it is equally decreased or increased respectively, without disturbing the congruence. Thus the tabulated scheme of numbers, including their equimultiples, represents any set of numbers such that each line (in scale r) is divisible by p, and the sum of any vertical pair is constant; the initial number determines practically the whole sequence.

Again, the number $111\ldots1$ (f figures) $\equiv 0 \pmod{p}$ in all cases for which the general congruence has been demonstrated. Hence any number may be added to each number of the right-hand or left-hand set of f terms without affecting the congruence.

Moreover, if f be even, the sum of the odd terms of (B)

$$\equiv \frac{1}{m-1}\left\{m^2\frac{m^{2f}-1}{m^4-1} - m\frac{m^f-1}{m^2-1}\right\}$$

$$\equiv 0 \pmod{p},$$

if p is also prime to r^2+1 and $f > 4$. Therefore, if f is an even number greater than 4, either the odd or the even terms in (B) may be replaced by zero, and then all the f numbers may be increased by the addition of any constant integer, and the congruence will still hold true, p being prime to $r-1$, r, $r+1$, and r^2+1, or having no common factor with either except a factor of f.

Further, if f is even and greater than 2, and therefore in the above case where $f > 4$, the number

$$1010\ldots \text{(to } f \text{ figures)} \equiv 0 \pmod{p},$$

as also to $f-1$ figures. Therefore, if f is even and greater than 4, the alternative terms, odd or even, may be replaced not only by zero but by any chosen integer, and the other set may have any constant integer added to each of its numbers without vitiating the congruence.

More generally, if f is a multiple of g, say ng, and h any integer not greater than g, the sum of every g^{th} term in (B) starting with $r^{f-h}\dfrac{m^h-1}{m-1}$

$$\equiv \frac{1}{m-1}\{m^h(m^h-1) + m^{h+g}(m^{h+g}-1) + \ldots + m^{h+(n-1)g}(m^{h+(n-1)g}-1)\}$$

$$\equiv \frac{1}{m-1}\left\{m^{2h}\frac{m^{2f}-1}{m^{2g}-1} - m^h\frac{m^f-1}{m^g-1}\right\}$$

$$\equiv 0 \pmod{p},$$

unless $n=1$ or 2, provided p is prime to $r^{2g}-1$, or, if there is a common factor, it is also a factor of n and r^g-1, or $2n$ and r^g+1, *i.e.*, when r is even; a factor of n in either case. Also

1000...1000... (n sets of 1 followed by $g-1$ zeros) $\equiv 0 \pmod{p}$,

unless $n=1$, provided p is either prime to r^g-1 *or* has a common factor with it and n.

Therefore any set of successive g^{th} terms may be replaced not only by zero but by any selected number throughout, provided n is not less than 3; or it may have any constant integer added to each of its n members, and the congruence will remain unaffected if p fulfils the condition of (i) being prime to $r^{2g}-1$, or having (ii) a factor common with r^g-1 and n, or (iii) a factor common with r^g+1 and $2n$, and therefore again with n if r is even.

Let g be the exponent to which r appertains (mod q). Take ng terms ($n>1$) of the set formed with a modulus q, the numbers thus recurring n times; their sum will be divisible by p as well as q, p being prime to r^g-1, or having a factor in common with it and with n. Even if g is not such an exponent, but is for some other reason such a number that the g^{th} term $\equiv 0 \pmod{q}$, as may be when the corresponding exponent is 1 or 2 (to be presently proved), then also the sum of f (*i.e.*, ng) terms, in which the first g numbers are repeated n times, will be divisible by p, though not necessarily by q.

§ 3. The cases when $f=1$ or 2 may be further considered.

(i) If $r\equiv 1 \pmod{q}$, we have $m=1$, and the g^{th} term in series (A) is $g\equiv 0 \pmod{q}$ when g is equal to q or any multiple of it. The sum of g terms $\equiv \tfrac{1}{2}g(g+1)$. This is congruent with zero if $g=q$ and q is odd, and if $g=2q$ when q is even.

If $nq=f$, the exponent to which r appertains (mod p), then the sum of f terms of the above series is divisible by p, provided any common factor of p and r^q-1 is also a factor of n; it is generally divisible by q only if q is odd. For example, $10\equiv 1 \pmod{3}$; the sum of three terms of corresponding series (A) is divisible by 3, since this is an odd number; and, taking $n=2$, the sum of 6 terms, or 2 periods, is divisible not only by 3 but also by any modulus for which 6 is the exponent to which 10 appertains, *i.e.*, by any factor of 10^6-1, which has not a factor common with 10^3-1, *i.e.*, it is divisible by 7, 11, and 13, which are the only factors which satisfy these conditions. Or we may consider the case of $5\equiv 1 \pmod{4}$,

where, in general, the sum of four terms (scale 5) is not divisible by 4, but the sum of eight terms is so divisible; and, therefore, the sum of sixteen terms is divisible by 4, and also by p, where $5^{16} \equiv 1 \pmod{p}$, 16 being the exponent appertaining to 5, and p having no factor common with 5^8-1, except 2 (*i.e.*, n); for instance, p may be 17 or 34, and the sum is is divisible by 136.

(ii) If $r^2 \equiv 1 \pmod{q}$, we have $m \equiv r$ not $\equiv 1$, and

$$(m-1)(m+1) \equiv 0.$$

Therefore, if q be any prime number, or 4, or any power or double any power of an odd number, we must have $m=q-1$ and $r \equiv -1$. Other values of q will lead to different formula for m as follows:—

If q be four times any prime or power of a prime, $m=\frac{1}{2}q-1$ and $r=(n+\frac{1}{2})q-1$, where n is any integer.

If $q=3(3q_1 \pm 1)$, where $(3q_1 \pm 1)$ is any power of an odd prime, it will be found that

$$m=3q_1 \pm 2=\tfrac{1}{3}q \pm 1 \text{ and } r=(n+\tfrac{1}{3})q \pm 1.$$

If $\qquad q=q_1^2-1,\ m=q_1=\sqrt{(q+1)}$.

When g is even the sum of g terms of the series (A)

$$\equiv r^{g-1}+(m+1)r^{g-2}+(m+2)r^{g-3}+2(m+1)r^{g-4}+\ldots$$
$$+\{(\tfrac{1}{2}g-1)m+\tfrac{1}{2}g\}r+\tfrac{1}{2}g(m+1).$$

In general, the last term $\equiv 0$ when $g=\dfrac{2q}{m+1}$, provided $m+1$ is a factor of q; if this proviso is not satisfied, $m+1$ and q must at least have a common factor, otherwise $m \equiv 1 \pmod{q}$; if, then, q_1 be the factor of q which is not a factor of $m+1$, the last term $\equiv 0$ when $g=2q_1$. Thus

(a) $m=q-1$, the 2nd and all even terms have zero residues, and the odd coefficients have a constant value 1;

(b) $m=\frac{1}{2}q-1$, every 4th term has zero residue;

(c) $m=\frac{1}{3}q-1$, every 6th term has zero residue;

(d) $m=\frac{1}{3}q+1$, every $\frac{2}{3}q$th term has zero residue;

(e) $m=\sqrt{(q+1)}$, every $2(m-1)$th term has zero residue.

The sum of g terms $=S$

$$\equiv m+(m+1)+(2m+1)+2(m+1)+\ldots+(\tfrac{1}{2}gm+\tfrac{1}{2}g-1)+\tfrac{1}{2}g(m+1)$$
$$\equiv \tfrac{1}{2}g\{(\tfrac{1}{2}g+1)m+\tfrac{1}{2}g\}.$$

If
$$g=\frac{2q}{m+1}, \qquad S\equiv q-\frac{q}{m+1},$$

and to obtain a series whose sum is congruent with zero this must be repeated $m+1$ times, *i.e.*, to $2q$ terms in all.

If $g=2q_1$ (as above), $S\equiv q-q_1$, which needs to be repeated q/q_1 times to make the sum congruent with zero, *i.e.*, to $2q$ terms, as before.

In the particular cases mentioned above, to obtain sum congruent with zero $(\text{mod}\, q)$,

(a) repeat q times, (b) repeat $\frac{1}{2}q$ times, (c) repeat $\frac{1}{3}q$ times,

(d) repeat 3 times, (e) repeat $m+1$ times.

If, then, g, being even, is the number of the first term congruent with zero $(\text{mod}\, q)$, the sum of ng (or f) terms is divisible by p, where f is the exponent to which r appertains $(\text{mod}\, p)$. And the same sum of f terms will only be also divisible by q when $f=2q$ or a multiple of $2q$.

§ 4. Special interest attaches to the cases in which r is of the form n^2+1, including the decimal scale of notation. In such a scale take $p=n^2\pm n+1$, or their product n^4+n^2+1. Then
$$r^6\equiv 1 \quad (\text{mod}\, p),$$

and 6 is the exponent to which r appertains.

Hence the sum of six terms of the series (A) formed with the modulus q is divisible by p in the following cases:

(1) If $q=p$.

(2) If $r\equiv 1$ $(\text{mod}\, q)$ and q, being odd, is a factor of 6, *i.e.*, if $q=3$, as in the scale of $9n^2+1$, *e.g.*, 10, 37, 82, &c.

Here a period of three figures is repeated, and the sum of six terms is divisible by pq, *i.e.*, by $3p$.

(3) If $r^2\equiv 1$ $(\text{mod}\, q)$, 2 being the exponent to which r appertains, so that q is not a factor of $r-1$.

Here a period of two figures recurs, since 2 is the only even factor of 6 which is less than 6; and the sum in question is divisible by p. If the number of six figures is divisible by q as well as by p, $6=2q$, therefore $q=3$. This occurs when $r^2\equiv 1$ (mod 3) and $r-1$ is prime to 3, *i.e.*, when r is not of the form $9n^2+1$, *i.e.*, in the scales of notation not included in (2) above. Then the sum of six terms is divisible by $3p$, if p is prime to 3.

(4) If $r^3 \equiv 1 \pmod{q}$, 3 being the exponent to which r appertains.

Here the period of three figures, which is divisible by q, is repeated, and the sum of six terms is divisible by pq. Here q may be any factor of r^3-1, which is not a factor of $r-1$ or r^2-1, and the only factor it can have in common with $r-1$ or r^2-1 is f, *i.e.*, 3. In the scale of 10, q may be any factor of 999 excepting 3 and multiples of 9, *i.e.*, it may be 37 or 111.

§ 5. In the scale of 10 the resulting number (A) to six figures, with modulus q,

(1) when $q=p$ (7, 13, or 91), is divisible by p;

(2) when $q=3$, is divisible by 3×1001, *i.e.*, 3, 7, 11, 13;

(3) when $q=11$, is divisible by 10101, *i.e.*, 3, 7, 13, 37;

(4) when $q=37$, is divisible by 37×1001, *i.e.*, 7, 11, 13, 37;

(5) when $q=111$, is divisible by 111×1001, *i.e.*, 3, 7, 11, 13, 37.

In all the above cases the number consisting of six figures is divisible by 7, except when p is 13. Thus there are six values of the modulus such that the resulting number is divisible by 7, but only two of them (viz., 7 and 91) without a recurring period of two or of three figures.

END OF VOL. XLI.

METCALFE AND CO. LIMITED, PRINTERS, TRINITY STREET, CAMBRIDGE.